BlackBerry Enterprise Solution

Version: 5.0 | Service Pack: 1

Security Technical Overview

BlackBerry

SWD-847262-1028044248-001

Contents

1 Overview 9
BlackBerry Enterprise Solution security 9
Security features of the BlackBerry Enterprise Solution 10
Architecture: BlackBerry Enterprise Solution 11

2 New in this release 16

3 Keys on a BlackBerry device 17
Device transport keys 18
States for device transport keys 18
Where the BlackBerry Enterprise Solution stores device transport keys 19
Generating device transport keys 20
Process flow: Generating a device transport key using BlackBerry Desktop Software version 4.0 or later 22
Process flow: Generating a device transport key using a BlackBerry Desktop Software version or BlackBerry Enterprise Server version that is earlier than version 4.0 23
Message keys 24
Process flow: Generating a message key on a BlackBerry Enterprise Server 24
Process flow: Generating a message key on a BlackBerry device 25
Content protection keys 25
Process flow: Turning on content protection using a BlackBerry Enterprise Server 26
Process flow: Generating a content protection key on a BlackBerry device 26
Process flow: Deriving an ephemeral key that protects a content protection key and ECC private key 27
Principal encryption keys 27
Process flow: Generating a principal encryption key 28
PIN encryption keys 28

4 Encrypting data that the BlackBerry Enterprise Server and a BlackBerry device send to each other 29
Algorithms that the BlackBerry Enterprise Solution uses to encrypt data 29
How the BlackBerry Enterprise Solution uses AES to encrypt data 29
How the BlackBerry Enterprise Solution uses Triple DES to encrypt data 31
Process flow: Sending an email message to a BlackBerry device using BlackBerry transport layer encryption 31
Process flow: Sending an email message from a BlackBerry device using BlackBerry transport layer encryption 32

5 Managing BlackBerry Enterprise Solution security 33
Using an IT policy to manage BlackBerry Enterprise Solution security 33

Using IT policy rules to manage BlackBerry Enterprise Solution security 33
Sending an IT policy over the wireless network 34
Using IT administration commands to protect a lost or stolen BlackBerry device 34
Process flow: Sending the Specify new device password and lock device IT administration command when content protection is turned on 35
Managing BlackBerry device access to the BlackBerry Enterprise Server 36
Using a segmented network architecture to prevent the spread of malware 37
Moving a BlackBerry device to a BlackBerry Enterprise Server that uses a different BlackBerry Configuration Database 37
Best practice: Controlling which applications can use the GPS feature on a BlackBerry device 37

6 BlackBerry device memory 39
Changing when a BlackBerry device cleans the BlackBerry device memory 39
When a BlackBerry device overwrites data in the BlackBerry device memory 40
Deleting all device data from the BlackBerry device memory 41
When a BlackBerry device deletes device data 41
Using IT policy rules to specify when a BlackBerry device must delete device data 42
Resetting a BlackBerry device to factory default settings 42
Process flow: Deleting all device data from a BlackBerry device 43
Scrubbing the memory of a BlackBerry device when deleting all BlackBerry device data 43
Scrubbing the BlackBerry device heap in RAM when deleting all BlackBerry device data 44
Scrubbing the flash memory on a BlackBerry device when deleting all BlackBerry device data 44
Scrubbing the user files on a BlackBerry device when deleting all BlackBerry device data 45

7 Protecting data on a BlackBerry device 46
Encrypting user data on a locked BlackBerry device 46
Configuring the encryption of BlackBerry device data on a locked BlackBerry device 46
Process flow: Encrypting user data on a locked BlackBerry device 47
Process flow: Decrypting user data on an unlocked BlackBerry device 47
Encrypting the device transport key on a locked BlackBerry device 48
What happens when a user resets a BlackBerry device after you turn on content protection for the device transport key 48
Resetting a BlackBerry device password when content protection is turned on 49
Process flow: Resetting a BlackBerry device password when content protection is turned on 49
Protecting passwords that a BlackBerry device stores 50
Protecting data that a BlackBerry device stores on a media card 51

Process flow: Generating an encryption key for a media card ... 51
How the BlackBerry Attachment Service protects data on a BlackBerry device ... 52
Best practice: Protecting the BlackBerry Attachment Service ... 52
How a BlackBerry device protects its operating system and the BlackBerry Device Software ... 52
How a BlackBerry device authenticates the boot ROM code and binds the BlackBerry device processor when the BlackBerry device turns on ... 52

8 Protecting the data that the BlackBerry Enterprise Solution stores in your organization's environment ... 54
Where the BlackBerry Enterprise Server stores messages and user data in the messaging environment ... 54
Data that the BlackBerry Configuration Database stores ... 54
Best practice: Protecting the data that the BlackBerry Configuration Database stores ... 55
How the BlackBerry Enterprise Solution protects IT policies ... 57

9 Protecting communication with a BlackBerry device ... 58
Opening a direct connection between a BlackBerry device and a BlackBerry Router ... 58
Process flow: Authenticating a BlackBerry device with the BlackBerry Enterprise Server using the BlackBerry Router protocol ... 58
Closing a direct connection between a BlackBerry device and BlackBerry Router ... 59
Impersonation attacks that the BlackBerry Router protocol is designed to prevent ... 59
How the BlackBerry Router protocol uses the Schnorr identification scheme to open an authenticated connection ... 59
Process flow: Using the BlackBerry Router protocol to close an authenticated connection ... 60
Process flow: Using the BlackBerry Router protocol to open an authenticated connection ... 60
Cryptosystem parameters that the BlackBerry Router protocol uses ... 62
Best practice: Protecting unsecured wireless messaging on the BlackBerry device ... 63
How the BlackBerry Enterprise Solution protects connections between a BlackBerry device and the Internet or intranet ... 64
Authenticating data that a BlackBerry device sends to the BlackBerry MDS Integration Service ... 64
Using SSL to connect to web services ... 65
Process flow: Registering a BlackBerry device with a BlackBerry MDS Integration Service ... 65
How a BlackBerry device protects a connection to a WAP gateway ... 66
Protecting HTTP connections from a BlackBerry device to content servers and application servers using HTTPS ... 66
What happens to data that is not delivered to a BlackBerry device ... 67
What happens to data that is not delivered because the connection between a BlackBerry Enterprise Server and the BlackBerry Infrastructure closes ... 67

What happens to data that is not delivered because a BlackBerry device is not available on the wireless network 67

10 Protecting BlackBerry Enterprise Solution communications in your organization's environment 68
How a BlackBerry Enterprise Server and the BlackBerry Infrastructure authenticate with each other 68
What happens when a BlackBerry Enterprise Server and the BlackBerry Infrastructure open an initial connection 68
How the BlackBerry Enterprise Solution protects a TCP/IP connection between a BlackBerry Enterprise Server and the BlackBerry Infrastructure 69
Process flow: Authenticating a BlackBerry Enterprise Server with the BlackBerry Infrastructure 69
How a BlackBerry Enterprise Server and messaging server protect a connection to each other 70
How the BlackBerry Enterprise Server components and the BlackBerry MVS protect communication 71
How the BlackBerry Desktop Manager protects communication using the BlackBerry inter-process protocol 71
Process flow: Authenticating the application loader tool or Roxio Media Manager with the BlackBerry Desktop Software using the BlackBerry inter-process protocol 72
How the BlackBerry Collaboration Service protects the connections between the BlackBerry Collaboration Service and instant messaging server 72

11 Activating a BlackBerry device 73
Activating a BlackBerry device over the wireless network 73
Process flow: Activating a BlackBerry device over the wireless network 73

12 Enrolling certificates on a BlackBerry device over the wireless network 75
Process flow: Enrolling a certificate when the certification authority approves certificate requests automatically 75
Process flow: Enrolling a certificate when a certification authority administrator approves certificate requests 76
Process flow: Enrolling a certificate using an RSA certification authority 77

13 Protecting BlackBerry Device Software updates 79
Protecting BlackBerry Device Software updates over the wireless network 79
How the BlackBerry Enterprise Solution protects BlackBerry Device Software updates over the wireless network using encryption 79
How the BlackBerry Enterprise Solution protects BlackBerry Device Software updates over the wireless network using IT policies and content protection 79
Battery power requirements for BlackBerry Device Software updates over the wireless network 80
Process flow: Preparing to send a BlackBerry Device Software update over the wireless network 80
How a BlackBerry device validates a BlackBerry Device Software update over the wireless network 80

Updating the BlackBerry Device Software from an update web site 80
Protecting cryptographic services data when updating the BlackBerry Device Software from an update web site 81
Process flow: Generating a BlackBerry services key that protects cryptographic services data 82
Process flow: Backing up cryptographic services data using the BlackBerry Desktop Manager 82
Process flow: Restoring cryptographic services data using the BlackBerry Desktop Manager or BlackBerry Application Web Loader 83

14 Extending messaging security to a BlackBerry device 84
Extending messaging security using PGP encryption 84
PGP public keys and PGP private keys 84
Retrieving PGP keys from a PGP Universal Server, LDAP servers, or DSML certificate servers 85
Encryption algorithms that the BlackBerry device supports for PGP encryption 85
Process flow: Sending an email message using PGP encryption 86
Process flow: Receiving a PGP encrypted message 87
Extending messaging security using S/MIME encryption 87
S/MIME certificates and S/MIME private keys 88
Retrieving S/MIME certificates and checking certificate status 89
S/MIME encryption algorithms 89
Process flow: Sending an email message using S/MIME encryption 90
Process flow: Receiving an S/MIME-encrypted email message 91
Extending messaging security using IBM Lotus Notes encryption 91
Protecting the password for an IBM Lotus Notes .id file 92
Process flow: Sending an email message using IBM Lotus Notes encryption 93
Process flow: Receiving an IBM Lotus Notes encrypted message 94
Extending messaging security to attachments 94
Process flow: Viewing an attachment in a PGP encrypted message or S/MIME-encrypted message 95
Process flow: Viewing an attachment that is encrypted using S/MIME encryption, PGP/MIME encryption, or OpenPGP encryption 95

15 Configuring two-factor authentication and protecting Bluetooth connections 96
BlackBerry Smart Card Reader 96
Advanced Security SD cards 96
Two-factor authentication 97
Verifying that a BlackBerry device is bound to a smart card 97
Process flow: Turning on two-factor authentication using a smart card 98

Creating two-factor authentication methods ... 98
Two-factor content protection ... 99
Unbinding a smart card from a BlackBerry device ... 99
Protecting Bluetooth connections on a BlackBerry device ... 100
Using CHAP to open a Bluetooth connection between the BlackBerry Desktop Software and a BlackBerry device ... 100

16 Wi-Fi enabled BlackBerry devices ... 101
Types of Wi-Fi networks ... 101
Security features of a Wi-Fi enabled BlackBerry device ... 102
Protecting a connection between a Wi-Fi enabled BlackBerry device and an enterprise Wi-Fi network ... 104
How a Wi-Fi enabled BlackBerry device can connect to the BlackBerry Infrastructure ... 104
How an SSL connection between a Wi-Fi enabled BlackBerry device and the BlackBerry Infrastructure protects data ... 105
Process flow: Opening an SSL connection between the BlackBerry Infrastructure and a Wi-Fi enabled BlackBerry device ... 105
Cipher suites that a Wi-Fi enabled BlackBerry device supports for opening SSL connections and TLS connections ... 105
Managing how a BlackBerry device connects to an enterprise Wi-Fi network ... 107
How the BlackBerry Enterprise Solution protects sensitive Wi-Fi information ... 107
Using a VPN with a Wi-Fi enabled BlackBerry device ... 107
Permitting a Wi-Fi enabled BlackBerry device to log in to a VPN concentrator ... 108
Using a segmented network to reduce the spread of malware on an enterprise Wi-Fi network that uses a VPN ... 108
Using a captive portal to connect to an enterprise Wi-Fi network or Wi-Fi hotspot ... 109
Protecting a connection between a Wi-Fi enabled BlackBerry device and an enterprise Wi-Fi network using RSA authentication ... 109
Process flow: Generating a token code for a software token ... 109

17 Layer 2 security methods that a Wi-Fi enabled BlackBerry device supports ... 111
WEP encryption ... 111
PSK protocol ... 112
IEEE 802.1X standard ... 112
Caching a PMK when using the IEEE 802.1X standard ... 112
Process flow: Authenticating a Wi-Fi enabled BlackBerry device with an enterprise Wi-Fi network using the IEEE 802.1X standard ... 113

EAP authentication methods that a Wi-Fi enabled BlackBerry device supports 113
LEAP authentication 113
PEAP authentication 114
EAP-TLS authentication 114
EAP-TTLS authentication 114
EAP-FAST authentication 115
EAP-SIM authentication 115
Encryption keys that a Wi-Fi enabled BlackBerry device supports for use with layer 2 security methods 115
EAP authentication methods that a BlackBerry device supports the use of CCKM with 116
Using certificates with PEAP authentication, EAP-TLS authentication, or EAP-TTLS authentication 116

18 Protecting a third-party application on a BlackBerry device 117
Creating a third-party application for a BlackBerry device 117
Specifying the resources third-party applications can access on a BlackBerry device 117
Managing third-party applications on a BlackBerry device using application control policy rules 117
Managing BlackBerry Java Applications on a BlackBerry device using code signing 118
Permitting a third-party application to encode data on a BlackBerry device 119
Removing third-party applications when a user deletes all BlackBerry device data 119

19 RIM Cryptographic API 120
Cryptographic algorithms and cryptographic codes that the RIM Cryptographic API supports 120
Symmetric block algorithms that the RIM Cryptographic API supports 120
Stream encryption algorithms that the RIM Cryptographic API supports 120
Asymmetric encryption algorithms that the RIM Cryptographic API supports 121
Key agreement scheme algorithms that the RIM Cryptographic API supports 121
Signature scheme algorithms that the RIM Cryptographic API supports 121
Key generation algorithms that the RIM Cryptographic API supports 122
Message authentication codes that the RIM Cryptographic API supports 122
Message digest codes that the RIM Cryptographic API supports 122
TLS and WTLS protocols that the RIM Cryptographic API supports 122
Cipher suites for the key establishment algorithm that the RIM Cryptographic API supports 123
Symmetric algorithms that the RIM Cryptographic API supports 123
Hash algorithms that the RIM Cryptographic API supports 123
Limitations of RIM Cryptographic API support for cipher suites for the key establishment algorithm 124

20 Related resources 125

21 Glossary 127

22 Provide feedback 139

23 Legal notice 140

Overview

1

BlackBerry Enterprise Solution security

The BlackBerry® Enterprise Solution consists of various products and components that are designed to extend your organization's communication methods to BlackBerry devices. The BlackBerry Enterprise Solution is designed to protect data that is in transit at all points between a BlackBerry device and BlackBerry® Enterprise Server. To protect data that is in transit over the wireless network, the BlackBerry Enterprise Server and BlackBerry device use symmetric key cryptography to encrypt the data. Only the BlackBerry Enterprise Server and BlackBerry device can decrypt the data that they send between each other. The BlackBerry Enterprise Server is designed to prevent third parties, including wireless service providers, from accessing your organization's potentially sensitive information in a decrypted format.

The BlackBerry Enterprise Solution uses confidentiality, integrity, and authenticity, which are principles for information security, to help protect your organization from data loss or alteration.

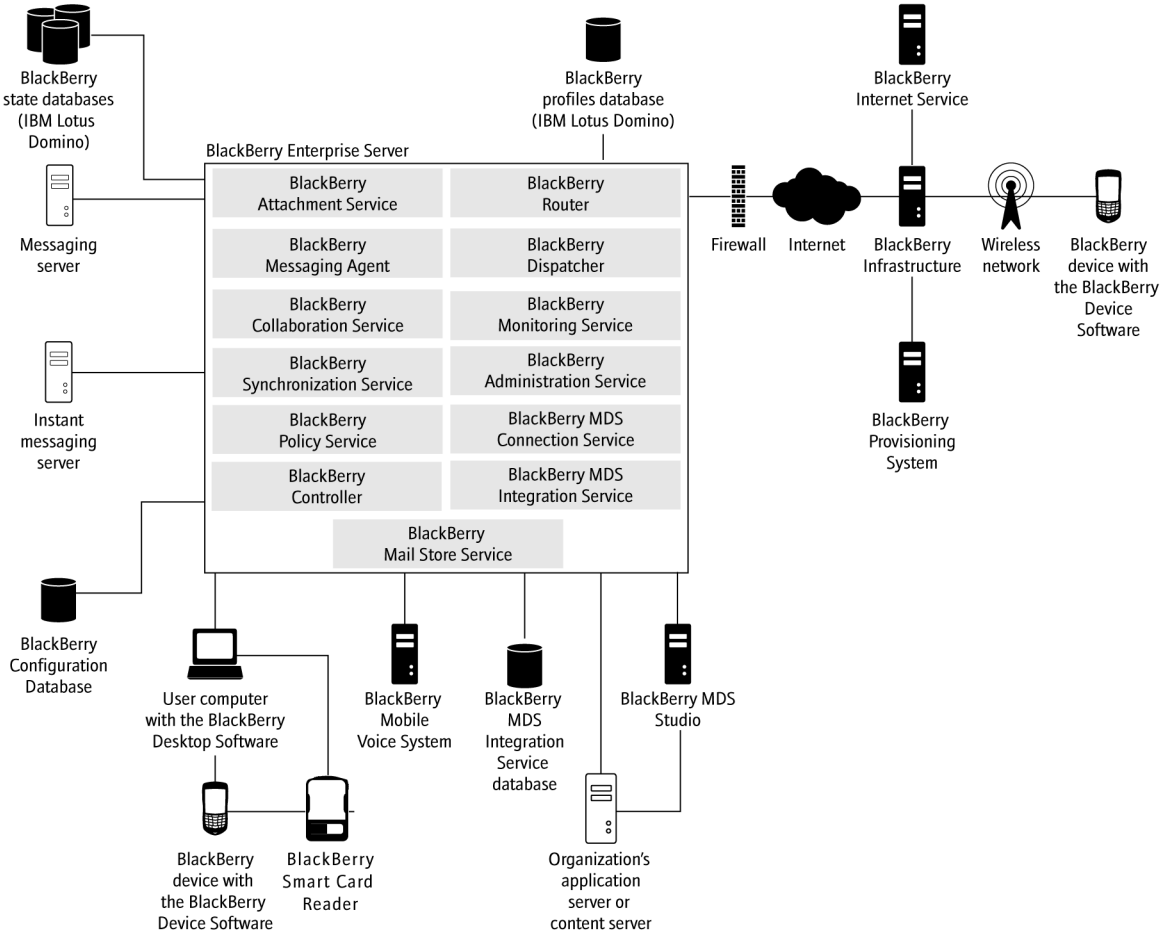
Principles	Description
confidentiality	The BlackBerry Enterprise Solution uses symmetric key cryptography to help make sure that only intended recipients can view the contents of email messages.
integrity	The BlackBerry Enterprise Solution uses symmetric key cryptography to help protect every email message that the BlackBerry device sends and to help prevent third parties from decrypting or altering the message data. Only the BlackBerry Enterprise Server and BlackBerry device know the value of the keys that they use to encrypt messages and recognize the format of a decrypted and decompressed message. The BlackBerry Enterprise Server or BlackBerry device reject a message automatically that is not encrypted with keys that they recognize as valid.
authenticity	Before the BlackBerry Enterprise Server sends data to the BlackBerry device, the BlackBerry device authenticates with the BlackBerry Enterprise Server to prove that the BlackBerry device knows the device transport key that is used to encrypt data.

Security features of the BlackBerry Enterprise Solution

Feature	Description
data protection	The BlackBerry® Enterprise Solution is designed to protect data that is in transit between the BlackBerry® Enterprise Server and a BlackBerry device and data that is in transit between your organization's messaging server and the email application on the user's computer. The BlackBerry Enterprise Solution encrypts data that is stored on the BlackBerry device and in the BlackBerry Configuration Database. To help protect data that is stored on the BlackBerry device, you can require a user to authenticate to the BlackBerry device using a password, a smart card, or both.
encryption key protection	The BlackBerry device is designed to protect the encryption keys that are stored on the BlackBerry device. The BlackBerry device encrypts the encryption keys when the BlackBerry device is locked.
control of BlackBerry device connections	The BlackBerry Enterprise Solution is designed to control the following connections: • connections using Bluetooth® technology to and from the BlackBerry device • connections from a Wi-Fi® enabled BlackBerry device to enterprise Wi-Fi networks The BlackBerry Enterprise Solution is designed to control which BlackBerry devices can connect to the BlackBerry Enterprise Server.
control of the behavior of the BlackBerry device and BlackBerry® Desktop Software	To control the behavior of the BlackBerry device and BlackBerry Desktop Software, you can send IT administration commands, IT policies, and application control policies to the BlackBerry device. You can use IT administration commands, IT policies, and application control policies to perform the following actions: • You can send IT administration commands to delete application data from the BlackBerry device and to lock the BlackBerry device. • You can send an IT policy to a BlackBerry device to change security settings. You can use the IT policy to enforce the BlackBerry device password and BlackBerry® Smart Card Reader password. • You can send an application control policy to a BlackBerry device to control whether third-party applications are available and can connect to the BlackBerry device.

Architecture: BlackBerry Enterprise Solution

The BlackBerry® Enterprise Solution consists of various components that permit you to extend your organization's communication methods to BlackBerry devices.



Component	Description
BlackBerry Administration Service	The BlackBerry Administration Service is a BlackBerry® Enterprise Server component that connects to the BlackBerry Configuration Database. You can use the BlackBerry Administration Service to manage BlackBerry Enterprise Server components, user accounts, and features for a BlackBerry device.
BlackBerry Attachment Service	The BlackBerry Attachment Service is a BlackBerry Enterprise Server component that converts supported message attachments into a format that the user can view on a BlackBerry device.
BlackBerry Collaboration Service	The BlackBerry Collaboration Service is a BlackBerry Enterprise Server component that provides a connection between your organization's instant messaging server and the collaboration client on a BlackBerry device.
BlackBerry Configuration Database	The BlackBerry Configuration Database is a relational database that contains configuration information that BlackBerry Enterprise Server components use. The BlackBerry Configuration Database stores the following information: • details about the connection from a BlackBerry Enterprise Server to the wireless network • contact list • address mappings between PINs and email addresses for BlackBerry MDS Connection Service push features • read-only copies of device transport keys, which encrypt the message keys that encrypt data that the BlackBerry Enterprise Server and BlackBerry device send between each other
BlackBerry Controller	The BlackBerry Controller is a BlackBerry Enterprise Server component that monitors other BlackBerry Enterprise Server components and restarts them if they stop responding.
BlackBerry® Desktop Software	The BlackBerry Desktop Software is an integrated suite of applications that a user installs on the user's computer. It manages the association between a BlackBerry device and the email account, synchronizes organizer data, calendar entries, and inboxes, and permits the user to download applications and BlackBerry® Device Software updates to a BlackBerry device.
BlackBerry device	A BlackBerry device provides the user with access to BlackBerry services such as messaging and browsing.

Component	Description
BlackBerry Device Software	The BlackBerry Device Software consists of applications on a BlackBerry device that permit the user to send and receive email messages, PIN messages, and text messages; manage calendar entries; and so on.
BlackBerry Dispatcher	The BlackBerry Dispatcher is a BlackBerry Enterprise Server component that compresses and encrypts all data that a BlackBerry device sends and receives. The BlackBerry Dispatcher sends the data through the BlackBerry Router, to and from the wireless network.
BlackBerry Enterprise Server	The BlackBerry Enterprise Server consists of various components that process, route, compress, encrypt, and send data over the wireless network to a BlackBerry device. The BlackBerry Enterprise Server is designed to open a two-way connection that is highly secure between the user's email account and the BlackBerry device. The BlackBerry Enterprise Server uses the connection to send email messages inside your organization's firewall.
BlackBerry® Infrastructure	The BlackBerry Infrastructure is designed to manage the wireless transport of messages between the wireless network and a BlackBerry device.
BlackBerry® Internet Service	The BlackBerry Internet Service provides a subscriber with messaging service and access to Internet content on a BlackBerry device.
BlackBerry Mail Store Service	The BlackBerry Mail Store Service connects to the messaging servers in your organization's environment and retrieves the contact information that the BlackBerry Administration Service requires to search for user accounts on the messaging servers.
BlackBerry MDS Connection Service	The BlackBerry MDS Connection Service is a BlackBerry Enterprise Server component that permits the user to access web content, the Internet, or your organization's intranet from a BlackBerry device. The BlackBerry MDS Connection Service also permits applications on a BlackBerry device to connect to your organization's application servers or content servers to retrieve application data and updates.
BlackBerry MDS Integration Service	The BlackBerry MDS Integration Service is a BlackBerry Enterprise Server component that provides application-level integration for BlackBerry® MDS Runtime Applications and BlackBerry® Browser Applications on BlackBerry devices. You can use the BlackBerry MDS Integration Service to install BlackBerry MDS Runtime Applications and BlackBerry Browser Applications on a BlackBerry device.
BlackBerry MDS Integration Service database	The BlackBerry MDS Integration Service database stores application data for the BlackBerry MDS Integration Service.

Component	Description
BlackBerry® MDS Studio	The BlackBerry MDS Studio can be used by your organization's developers to create BlackBerry MDS Runtime Applications and to publish the applications to the BlackBerry MDS Application Repository.
BlackBerry Messaging Agent	The BlackBerry Messaging Agent is a BlackBerry Enterprise Server component that connects to your organization's messaging server to provide messaging services, calendar management, contact lookups, attachment viewing, and attachment downloading. The BlackBerry Messaging Agent also generates device transport keys and acts as a gateway for the BlackBerry Synchronization Service to access organizer data on the messaging server. The BlackBerry Messaging Agent synchronizes configuration data between the BlackBerry Configuration Database and user mailboxes.
BlackBerry® Mobile Voice System	The BlackBerry MVS integrates your organization's PBX phone system with the BlackBerry Enterprise Server to extend desk phone features to a BlackBerry device.
BlackBerry Monitoring Service	The BlackBerry Monitoring Service is a BlackBerry Enterprise Server component that is designed to help you monitor your organization's BlackBerry Domain. You can use the BlackBerry Monitoring Service to troubleshoot issues and monitor the health of your organization's BlackBerry Domain proactively.
BlackBerry Policy Service	The BlackBerry Policy Service is a BlackBerry Enterprise Server component that sends IT policies and IT administration commands and provisions service books. The BlackBerry Policy Service sends service books to configure settings for features and components on a BlackBerry device.
BlackBerry profiles database	The BlackBerry profiles database is an IBM® Lotus® Domino® database that the BlackBerry® Enterprise Server for IBM® Lotus® Domino® uses to store configuration data for the user account.
BlackBerry® Provisioning System	The BlackBerry Provisioning System is designed to permit wireless service providers to configure and manage BlackBerry services for their subscribers. A wireless service provider can assign, activate, deactivate, suspend, and resume BlackBerry services and check the current status of service requests for a BlackBerry device on the wireless network.
BlackBerry Router	The BlackBerry Router is a BlackBerry Enterprise Server component that connects to the wireless network to send data to and from a BlackBerry device. The BlackBerry Router also sends data over your organization's network to a BlackBerry device that is connected to a computer that hosts the BlackBerry® Device Manager.

Component	Description
BlackBerry® Smart Card Reader	The BlackBerry Smart Card Reader controls access to your organization's sensitive communications using Bluetooth® technology and the latest encryption technologies. The BlackBerry Smart Card Reader permits an organization to use two-factor authentication.
BlackBerry state databases	The BlackBerry state databases are Lotus Domino databases that the BlackBerry Enterprise Server for IBM Lotus Domino uses to store data that associates email messages that a BlackBerry device sends or receives to corresponding messages in the user's email application. The data in the BlackBerry state databases supports features such as email message reconciliation, email message forwarding, email message filing, and replying with text.
BlackBerry Synchronization Service	The BlackBerry Synchronization Service is a BlackBerry Enterprise Server component that synchronizes organizer data between a BlackBerry device and your organization's messaging server over the wireless network.
instant messaging server	The instant messaging server stores instant messaging accounts.
messaging server	The messaging server receives, sends, and stores all email messages.
organization's application server or content server	Your organization's application server or content server provides push applications and intranet content that the BlackBerry MDS Services use to install on a BlackBerry device.

New in this release

2

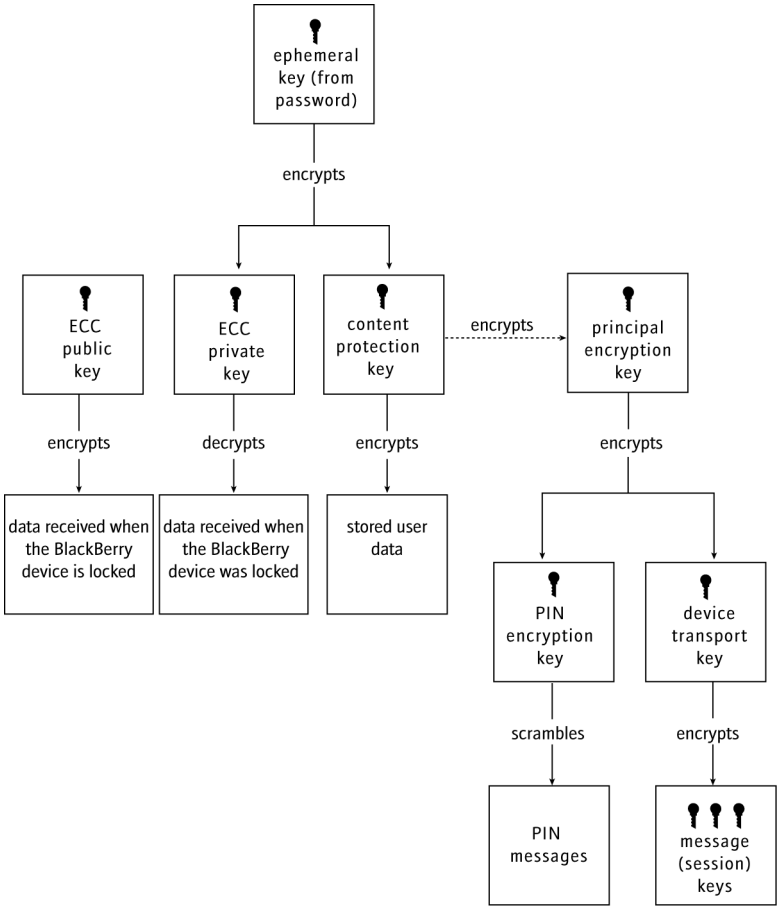
This document describes the security features that the BlackBerry® Enterprise Server version 5.0 SP1, BlackBerry® Desktop Software version 5.0, BlackBerry® Device Software version 5.0, and BlackBerry® Smart Card Reader version 2.0 support, unless otherwise stated.

Feature	Description
Advanced Security SD card support	Similar to the BlackBerry® Smart Card Reader, an Advanced Security SD card permits a user to use what the user has (smart card) and what the user knows (smart card password) to prove the user's identity to the BlackBerry device. The BlackBerry® Enterprise Solution supports Advanced Security SD cards that use the MCEX smart card security system.
DSML support	You can configure the BlackBerry MDS Connection Service to use DSML to search for and retrieve certificates from DSML certificate servers for BlackBerry devices that are running BlackBerry Device Software versions 5.0 and later.
NTLMv2 support	BlackBerry Enterprise Server version 5.0 SP1 and BlackBerry Device Software version 5.0 support using NTLMv2 to authenticate to content servers.
proximity authentication	Proximity authentication is an authentication method that permits a user to unlock a BlackBerry device using a BlackBerry device password and BlackBerry Smart Card Reader when the BlackBerry Smart Card Reader is located within Bluetooth® technology range of the BlackBerry device. Proximity authentication does not require the user to have a smart card. You can use proximity authentication with BlackBerry Smart Card Reader version 2.0.
two-factor content protection	Two-factor content protection requires a BlackBerry device password, a smart card, and an authentication certificate that is stored on a BlackBerry device to protect the content protection key. You can use two-factor content protection with BlackBerry Smart Card Reader version 2.0 or an Advanced Security SD card.
User Authenticator API	BlackBerry® Java® Development Environment version 5.0 includes the User Authenticator API that developers can use to create two-factor authentication methods that a user can use with the BlackBerry device password to unlock a BlackBerry device.

Keys on a BlackBerry device

3

The BlackBerry® Enterprise Solution generates keys that are designed to protect the data that is stored on a BlackBerry device and the data that the BlackBerry device and BlackBerry® Enterprise Server send between each other.



Key	Description
content protection key	The content protection key encrypts user data on the BlackBerry device when the BlackBerry device is locked.
device transport key	The device transport key encrypts the message keys.
ECC private key	The ECC private key decrypts data when the user unlocks the BlackBerry device.

Key	Description
ECC public key	The ECC public key encrypts the stored data that the BlackBerry device receives when the BlackBerry device is locked.
ephemeral key	The ephemeral key encrypts the ECC public key, ECC private key, and content protection key on the BlackBerry device.
PIN encryption key	The PIN encryption key scrambles PIN messages.
principal encryption key	If you or a user turns on content protection, the principal encryption key encrypts the device transport key and PIN encryption key that is specific to your organization when the BlackBerry device is locked.
message keys	The message keys (also known as session keys) encrypt data sent to and from the BlackBerry device.

Device transport keys

The device transport key encrypts the message keys that help protect the data sent between a BlackBerry® Enterprise Server and BlackBerry device. The BlackBerry Enterprise Server and BlackBerry device generate the device transport key when a user activates the BlackBerry device.

The BlackBerry Enterprise Server and BlackBerry device do not send the device transport key over the wireless network when they generate the device transport key or when they exchange messages.

The BlackBerry® Enterprise Solution is designed so that only the BlackBerry Enterprise Server and BlackBerry device know the value of the device transport key. The BlackBerry Enterprise Server and BlackBerry device reject a data packet if they do not recognize the format of a data packet or do not recognize the device transport key that protects the data packet.

States for device transport keys

The BlackBerry® Enterprise Solution generates device transport keys on a regular basis so that a potentially malicious user cannot access all data sent between a BlackBerry® Enterprise Server and BlackBerry device if that user compromises a device transport key. As the BlackBerry Enterprise Solution generates device transport keys, the device transport keys change state from pending to current to previous.

State	Description
pending	A pending device transport key is the device transport key that the BlackBerry Enterprise Solution generates to replace the current device transport key. If the user generates the device transport key using the BlackBerry® Desktop Software, the BlackBerry Desktop Software sends the pending device transport key to the BlackBerry device when the user connects the BlackBerry device to the computer. The messaging environment and BlackBerry Configuration Database store the pending device transport key.
current	A current device transport key is the device transport key that the BlackBerry device currently uses to encrypt and decrypt message keys.
previous	A previous device transport key is the device transport key that the BlackBerry device used before the BlackBerry Enterprise Solution generated the current device transport key. The BlackBerry device stores previous device transport keys in flash memory for 7 days. The BlackBerry device stores previous device transport keys so that a user can decrypt messages even after the user generates a new device transport key while messages are queued. The messaging server and BlackBerry Configuration Database store the previous device transport key that the BlackBerry Enterprise Server and BlackBerry device used most recently. A potentially malicious user cannot use the previous device transport key to learn the currrent device transport key. The BlackBerry Enterprise Server and BlackBerry device discard the key pair after they generate the device transport key. If a potentially malicious user compromises both the static private key and ephemeral private key for a device transport key, other device transport keys that the BlackBerry Enterprise Server and BlackBerry device generate are not compromised.

Where the BlackBerry Enterprise Solution stores device transport keys

The BlackBerry® Enterprise Solution stores current, pending, and previous device transport keys in the BlackBerry Configuration Database, in the messaging environment, and on each BlackBerry device.

A BlackBerry device stores the device transport keys in a key store database in flash memory. The key store database is designed to prevent a potentially malicious user from copying the device transport keys to a computer by trying to back up the device transport keys. A potentially malicious user cannot extract key data from flash memory.

To avoid compromising the device transport keys that are stored in the BlackBerry Configuration Database or in the messaging environment, you must protect the BlackBerry Configuration Database and the storage location of the device transport key in the messaging environment.

Messaging environment	Storage location on the messaging environment
IBM® Lotus® Domino®	BlackBerry profiles database
Microsoft® Exchange	mailbox of the email application on the user's computer
Novell® GroupWise®	—

Where the BlackBerry Enterprise Solution stores device transport keys in a Microsoft Exchange environment

In a Microsoft® Exchange environment, the BlackBerry® Enterprise Solution stores the device transport keys in a hidden folder that is named BlackBerryHandheldInfo. The BlackBerryHandheldInfo folder is located in a root folder of the mailbox for the user account on the Microsoft Exchange Server®. The BlackBerryHandheldInfo folder stores the following data:

- message of class `RIM.BlackBerry.Handheld.Config` that contains the user's configuration information, including the device transport key
- device transport keys in binary form with tags that indicate whether the status of the device transport keys is pending (0x6002 tag), current (0x6003 tag), or previous (0x6004 tag)

Where the BlackBerry Enterprise Solution stores the device transport keys in an IBM Lotus Domino environment

In an IBM® Lotus® Domino® environment, the BlackBerry® Enterprise Solution stores the device transport keys in a Lotus Domino database that is named BlackBerryProfiles.nsf. The BlackBerry profiles database contains configuration information for every user account that exists in the Data directory. The BlackBerry profiles database stores an account record that contains the RIMCurrentEncryptionKeyText field, RIMPendingEncryptionKeyText field, and RIMPreviousEncryptionKeyText field. The fields stores the device transport keys for every user account in a hexadecimal string using alphanumeric characters.

Generating device transport keys

Generating the first device transport key for a BlackBerry device during the activation process

If a user connects a BlackBerry® device to a computer for the first time and activates the BlackBerry device, the BlackBerry® Desktop Software generates the device transport key and sends it to the BlackBerry device and messaging server.

If a user activates the BlackBerry device over the wireless network, the BlackBerry® Enterprise Server and BlackBerry device negotiate to select the strongest algorithm that they both support (either AES or Triple DES) and use that algorithm to generate a device transport key. To generate public keys for key rollover on the BlackBerry device and create a strong, cryptographically protected connection between the BlackBerry Enterprise Server and BlackBerry device, the BlackBerry® Enterprise Solution uses the SPEKE authentication method and the activation password for the BlackBerry device.

For more information about the SPEKE authentication method, visit http://standards.ieee.org/ to read *Password-Based Public Key Cryptography (P1363.2)*.

Security characteristics for generating the first device transport key

Characteristics	Description
authentication and integrity	The wireless activation process verifies that only a user with the correct activation password can activate a BlackBerry® device that you associate with a BlackBerry® Enterprise Server.
prevention of offline dictionary attacks	The wireless activation process is designed so that a potentially malicious user cannot determine a user's password by viewing the protocol packets that the BlackBerry Enterprise Server and BlackBerry device send between each other.
prevention of online dictionary attacks	The wireless activation process is designed so that the BlackBerry Enterprise Server prevents a potentially malicious user from activating a BlackBerry device if that user types an incorrect activation password more than five times.
long-term public keys exchanged	The wireless activation process verifies that the BlackBerry Enterprise Server and BlackBerry device can exchange the device transport key in a manner that is designed to be highly secure when they generate a new device transport key.

Generating subsequent device transport keys for a BlackBerry device

By default, the BlackBerry® Enterprise Server and BlackBerry device generate subsequent device transport keys every 30 days. If a pending device transport key exists and a user connects a BlackBerry device to a computer, the current device transport key on the BlackBerry device becomes the previous device transport key and the pending device transport key becomes the current device transport key. If no pending device transport key exists, you, the user, or the BlackBerry® Desktop Software can generate a device transport key.

The BlackBerry Enterprise Server and BlackBerry device generate the device transport key using existing long-term public keys and the ECMQV key exchange algorithm to negotiate a device transport key. This method is designed so that a potentially malicious user is unable to calculate the device transport key. The BlackBerry Enterprise Server and BlackBerry device discard the key pair after they generate the device transport key.

For more information about the ECMQV key exchange algorithm, see *NIST: Special Publication 800-56: Recommendation on Key Establishment schemes, Draft 2.0* and the *Guide to Elliptic Curve Cryptography*.

Security characteristics for generating subsequent device transport keys

Characteristics	Description
authentication	Authentication means that only a BlackBerry® device that a user authenticates with or a BlackBerry® Enterprise Server can generate subsequent device transport keys. Authentication is designed so that a potentially malicious user cannot use another device to impersonate an activated BlackBerry device and generate a device transport key.
password independent	Password independent means that the user does not require an activation password and you do not have to perform any actions when you or a user generates a subsequent device transport key.
flexible initiation	Flexible initiation means that you or a user can generate a subsequent device transport key at any time.
PFS	PFS means that subsequent device transport keys are independent of previous device transport keys. A device transport key does not help the potentially malicious user decrypt data that another device transport key protects.

Generating a device transport key manually

To generate a device transport key on an activated BlackBerry® device, a user can click Regenerate Encryption Key, in the BlackBerry device options, in the security options. The BlackBerry device sends the request to generate a device transport key to the BlackBerry® Enterprise Server over the wireless network.

A user can also generate a device transport key using the BlackBerry® Desktop Manager. By default, the BlackBerry Enterprise Server sends a request to the BlackBerry Desktop Manager every 30 days to prompt the user to generate a new device transport key on the BlackBerry device, even if the user chooses to generate the device transport key manually using the BlackBerry Desktop Manager.

You can use the BlackBerry Administration Service to start the process to generate a new device transport key.

Process flow: Generating a device transport key using BlackBerry Desktop Software version 4.0 or later

In BlackBerry® Desktop Software version 4.0 or later, the process to generate a device transport key uses the current time and cursor movements as the seeds to generate random data.

To generate the device transport key, the BlackBerry Desktop Software performs the following actions:

1. prompts the user to move the cursor
2. uses the srand function of the C programming language to examine the lowest 12 bits of the x and y co-ordinates of the new cursor location
   If the bits are different from the previous sample, the BlackBerry Desktop Software stores the bits, which generates 3 bytes of randomness. If the bits are the same as the bits in the previous sample, the BlackBerry Desktop Software does not store any bits.
3. uses the srand function to examine the next bits, after the srand function waited for a random interval between 50 milliseconds and 150 milliseconds
   The srand function continues to wait for random intervals and examine bits until the BlackBerry Desktop Software stores 384 bytes of randomness.
4. retrieves 384 bytes of randomness from the Microsoft® Cryptographic API, for a total of 768 bytes
5. hashes the 384 bytes of randomness from the cursor co-ordinates and the 384 bytes of randomness from the Microsoft Cryptographic API with SHA-512 to produce 512 bits of data
6. frees the computer memory that is associated with the unused bits
7. generates the device transport key using the first 256 bits of data if the BlackBerry Desktop Software supports AES encryption, or the first 128 bits of data if the BlackBerry Desktop Software supports Triple DES encryption
8. deletes any bits of data that it does not use to generate the device transport key

Process flow: Generating a device transport key using a BlackBerry Desktop Software version or BlackBerry Enterprise Server version that is earlier than version 4.0

In BlackBerry® Enterprise Server or BlackBerry® Desktop Software versions that are earlier than version 4.0, the process that generates a device transport key uses the current time and the cursor movements as the seeds to generate random data.

1. The BlackBerry Desktop Software prompts the user to move the cursor.
2. The BlackBerry Enterprise Server or BlackBerry Desktop Software generates 2 bits or 4 bits when the user moves the cursor, depending on whether the cursor movement changed one or both of the x and y axes. The BlackBerry Enterprise Server or BlackBerry Desktop Software generates bit samples in this way until it accumulates at least 8 bits.
3. The srand function of the C programming language generates a random integer.
4. The BlackBerry Enterprise Server or BlackBerry Desktop Software performs the following actions:
   a. examines the least significant bit of the integer.
      If the bit is a 1, the BlackBerry Enterprise Server or BlackBerry Desktop Software stores the complement of 1 bit of the accumulated 8 bits. Otherwise, the BlackBerry Enterprise Server or BlackBerry Desktop Software stores the unmodified accumulated 8 bits. This process is designed to make sure that, even if a user can replicate a previous user's cursor movements, the resulting value is still unique.
   b. generates a sample of 256 random bits from the cursor movements of the user

c. uses the SHA-1 function to hash the 256 bits
d. generates the device transport key of the BlackBerry device using the first 128 bits of the hash

Message keys

A BlackBerry® Enterprise Server and BlackBerry device generate one or more message keys that are designed to protect the integrity of the data (for example, short keys or large messages) that the BlackBerry Enterprise Server and BlackBerry device send between each other. If a message exceeds 2 KB and consists of several data packets, the BlackBerry Enterprise Server and BlackBerry device generate a unique message key for each data packet.

Each message key consists of random data that is designed to make it difficult for a third party to decrypt, re-create, or duplicate the message key.

The message key is a type of session key. The BlackBerry Enterprise Server and BlackBerry device do not store the message keys but they free the memory that is associated with the message keys after the BlackBerry Enterprise Server or BlackBerry device uses the message keys to decrypt the message.

Process flow: Generating a message key on a BlackBerry Enterprise Server

A BlackBerry® Enterprise Server is designed to use the DSA PRNG function to generate a message key.

To generate a message key, the BlackBerry Enterprise Server performs the following actions:

1. retrieves random data from multiple sources for the seed, using a technique that the BlackBerry Enterprise Server derives from the initialization function of the ARC4 encryption algorithm
2. uses the random data to reorder the contents of a 256-byte state array (also known as a 2048-bit state array)
   If the Microsoft® Cryptographic API exists on the computer that hosts the BlackBerry Enterprise Server, the BlackBerry Enterprise Server requests 512 bits of randomness from the Microsoft Cryptographic API to increase the randomness of the data.
3. adds the 256-byte state array into the ARC4 algorithm to further randomize the 256-byte state array
4. draws 521 bytes from the 256-byte state array
   The BlackBerry Enterprise Server draws an additional 9 bytes for the 256-byte state array, for a total of 521 bits (512 + 9 = 521) to make sure that the pointers before and after the generation process are not in the same place, and in case the first few bytes of the 256-byte state array are not random.
5. uses SHA-512 to hash the 521-byte value to 64 bytes
6. uses the 64-byte value to seed the DSA PRNG function
   The BlackBerry Enterprise Server stores a copy of the seed in a file. When the BlackBerry Enterprise Server restarts, it reads the seed from the file and uses the XOR function to compare the stored seed with the new seed.
7. uses the DSA PRNG function to generate 256 pseudo-random bits for use with AES encryption and 128 pseudo-random bits for use with Triple DES encryption

8. uses the pseudo-random bits with AES encryption or Triple DES encryption to generate the message key

For more information about the DSA PRNG function, see *Federal Information Processing Standard - FIPS PUB 186-2*.

Process flow: Generating a message key on a BlackBerry device

A BlackBerry® device is designed to use the DSA PRNG function to generate a message key.

To generate a message key, the BlackBerry device performs the following actions:

1. retrieves random data from multiple sources to generate the seed using a technique that the BlackBerry device derives from the initialization function of the ARC4 encryption algorithm
2. uses the random data to reorder the contents of a 256-byte state array (also known as a 2048-bit state array)
3. adds the 256-byte state array into the ARC4 encryption algorithm to further randomize the 256-byte state array
4. draws 521 bytes from the ARC4 state array
   The BlackBerry device draws an additional 9 bytes for the 256-byte state array, for a total of 521 bytes (512 + 9 = 521) to make sure that the pointers before and after the call are not in the same place, and in case the first few bytes of the ARC4 state array are not random.
5. uses SHA-512 to hash the 521-byte value to 64 bytes
6. uses the 64-byte value to seed the DSA PRNG function
   The BlackBerry device stores a copy of the seed in a file. When the BlackBerry device restarts, it reads the seed from the file and uses the XOR function to compare the stored seed with the new seed.
7. uses the DSA PRNG function to generate 128 pseudo-random bits for use with Triple DES encryption and 256 pseudo-random bits for use with AES encryption
8. uses the pseudo-random bits with Triple DES encryption or AES encryption to generate the message key

For more information about the DSA PRNG function, see *Federal Information Processing Standard - FIPS PUB 186-2*.

Content protection keys

When you or a user turns on content protection for a BlackBerry® device, the BlackBerry device generates a content protection key. The content protection key is designed to encrypt user data on the BlackBerry device when it is locked.

When the BlackBerry device is locked, an encryption process begins. The BlackBerry device frees the memory that it associates with the content protection key and ECC private key that it stores in RAM. The BlackBerry device then uses the ECC public key to encrypt new data that it receives.

When a user unlocks a BlackBerry device, the BlackBerry device decrypts the content protection key and ECC private key in flash memory. When the user wants to view data, the BlackBerry device uses the content protection key or ECC private key to decrypt the data before the BlackBerry device displays it. An unlocked BlackBerry device uses the content protection key to encrypt new data that the user types or adds to the BlackBerry device, or that the BlackBerry device receives.

Process flow: Turning on content protection using a BlackBerry Enterprise Server

You can turn on content protection using a BlackBerry® Enterprise Server when you configure the Content Protection Strength IT policy rule.

1. The BlackBerry Enterprise Server performs the following actions:
   a. selects *b* randomly
   b. calculates $B = bP$
   c. stores *b* in the BlackBerry Configuration Database
   d. sends *B* in the IT policy to the BlackBerry device
2. The BlackBerry device performs the following actions:
   a. verifies that *B* is a valid public key
   b. selects *d* randomly
   c. calculates $D = dP$
   d. stores *D* in flash memory
   e. calculates $K = dB$
   f. uses *K* to encrypt the current BlackBerry device password
   g. uses the encrypted BlackBerry device password to encrypt the content protection key
   h. permanently deletes *d* and *K*

When the BlackBerry device permanently deletes *d*, the BlackBerry device is designed so that a potentially malicious user cannot use the data that remains on the BlackBerry device to recover *K*. Only the BlackBerry Enterprise Server knows *b* and can recalculate $K = dB = dbP = bD$ if it is provided with *d*.

Process flow: Generating a content protection key on a BlackBerry device

When you or a user turns on content protection on the BlackBerry® device for the first time, the BlackBerry device performs the following actions:

1. uses a DSA PRNG function to randomly generate a content protection key
2. generates an ECC key pair with a bit length that you or the user determines
3. prompts the user to type the BlackBerry device password
4. derives an ephemeral key that uses AES-256 encryption from the BlackBerry device password, using PKCS #5
5. uses the ephemeral key to encrypt the content protection key and ECC private key
6. stores the encrypted content protection key, encrypted ECC private key, and ECC public key in flash memory

The content protection key is a semi-permanent key that uses AES-256 encryption. If the user changes the BlackBerry device password, the BlackBerry device uses the new password to derive a new ephemeral key. The BlackBerry device uses the new ephemeral key to re-encrypt the versions of the content protection key and ECC private key that are in flash memory.

For more information about the DSA PRNG function, see *Federal Information Processing Standard - FIPS PUB 186-2*. For more information about PKCS #5, visit www.rsa.com to see *PKCS #5: Password-Based Cryptography Standard*.

Process flow: Deriving an ephemeral key that protects a content protection key and ECC private key

A BlackBerry® device uses an ephemeral key to encrypt a content protection key and ECC private key. The BlackBerry device derives the ephemeral key, which is an AES-256 encryption key, from the BlackBerry device password using PKCS #5.

To derive an ephemeral key, the BlackBerry device performs the following actions:

1. selects a 64-bit salt (which is random data that the BlackBerry device mixes with the BlackBerry device password) The salt prevents two identical passwords from turning into the same key.
2. concatenates the salt, password, and salt again into a byte array (for example, `Salt|Password|Salt`)
3. hashes the byte array with SHA-256
4. stores the resulting hash in a byte array that is called a key

```
(key) =
SHA256(Salt|Password|Salt)
```

5. hashes the key 18 more times and stores the result in the key each time
   For example, for i=0 to 18, the BlackBerry device performs the following actions:

```
(key) = SHA256(key)
 i++
 done
```

The final hash creates the ephemeral key.

For more information, visit www.rsa.com to see *PKCS #5: Password-Based Cryptography Standard*.

Principal encryption keys

When you or a user turns on content protection for device transport keys, a BlackBerry® device generates a principal encryption key and stores it in flash memory. The BlackBerry device uses the principal encryption key to encrypt the device transport keys that are stored on the BlackBerry device in flash memory and the PIN encryption key that is specific to your organization. The BlackBerry device encrypts the principal encryption key using the content protection key. When the BlackBerry device receives data that the device transport key encrypts while the BlackBerry device is locked, the BlackBerry device uses the principal encryption key to decrypt the device transport key that is in flash memory.

Process flow: Generating a principal encryption key

When you or a user turns on content protection for device transport keys on a BlackBerry® device for the first time, the BlackBerry device performs the following actions:

1. generates a principal encryption key, which is an AES-256 encryption key
2. stores the decrypted principal encryption key in RAM
3. uses the existing content protection key to encrypt the principal encryption key
4. stores the encrypted principal encryption key in flash memory

When the BlackBerry device locks, the BlackBerry device uses the decrypted principal encryption key to encrypt the device transport keys that are stored in the flash memory of the BlackBerry device.

PIN encryption keys

A PIN identifies each BlackBerry® device and BlackBerry enabled device on the wireless network. If a user knows the PIN of another BlackBerry device, the user can send a PIN message to the BlackBerry device. Unlike a message that a user sends to an email address, a PIN message bypasses the BlackBerry® Enterprise Server and your organization's network.

The BlackBerry device scrambles PIN messages using the PIN encryption key. By default, each BlackBerry device uses a global PIN encryption key, which allows the BlackBerry device to decrypt every PIN message that the BlackBerry device receives. Your organization can use a global PIN encryption key, a PIN encryption key that is specific to your organization, or both.

During the manufacturing process, Research In Motion adds a global PIN encryption key to the BlackBerry device. To permit a BlackBerry device to receive and decrypt PIN messages in your organization only, you can generate a PIN encryption key that is specific to your organization. A BlackBerry device that has a PIN encryption key that is specific to your organization can send and receive PIN messages with other BlackBerry devices on your organization's network that use the same PIN encryption key. The BlackBerry device scrambles the PIN messages using a PIN encryption key that is specific to your organization instead of using the global PIN encryption key.

You can configure the Firewall Block Incoming Messages IT policy rule to limit the number of BlackBerry devices in your organization that can receive PIN messages that use the PIN encryption key that is specific to your organization, the global PIN encryption key, or both.

You can generate a new PIN encryption key using the BlackBerry Administration Service if you know that the current PIN encryption key is compromised. You can update the PIN encryption key and send it to user accounts using the BlackBerry Administration Service.

Encrypting data that the BlackBerry Enterprise Server and a BlackBerry device send to each other 4

To encrypt data that is in transit between the BlackBerry® Enterprise Server and a BlackBerry device in your organization, the BlackBerry® Enterprise Solution uses BlackBerry transport layer encryption. BlackBerry transport layer encryption is designed to encrypt data from the time that a BlackBerry device user sends a message from the BlackBerry device to when the BlackBerry Enterprise Server receives the message, and from the time that the BlackBerry Enterprise Server sends a message to when the BlackBerry device receives the message.

Before the BlackBerry device sends a message, it compresses and encrypts the message using the device transport key. When the BlackBerry Enterprise Server receives a message from the BlackBerry device, the BlackBerry Dispatcher decrypts the message using the device transport key, and then decompresses the message.

Algorithms that the BlackBerry Enterprise Solution uses to encrypt data

The BlackBerry® Enterprise Solution uses AES or Triple DES as the symmetric key cryptographic algorithm for encrypting data. By default, the BlackBerry® Enterprise Server uses the strongest algorithm that both the BlackBerry Enterprise Server and the BlackBerry device support for BlackBerry transport layer encryption.

If you configure the BlackBerry Enterprise Server to support AES and Triple DES, by default, the BlackBerry Enterprise Solution generates device transport keys using AES encryption. If a BlackBerry device uses BlackBerry® Device Software version 3.7 or earlier or BlackBerry® Desktop Software version 3.7 or earlier, the BlackBerry Enterprise Solution generates the device transport keys of the BlackBerry device using Triple DES.

How the BlackBerry Enterprise Solution uses AES to encrypt data

By default, when a BlackBerry® device supports AES, the BlackBerry® Enterprise Solution uses AES for BlackBerry transport layer encryption. The BlackBerry Enterprise Solution uses AES in CBC mode to generate the message keys and device transport keys. The keys consist of 256 bits of data.

BlackBerry® Enterprise Server version 4.0 or later, BlackBerry® Device Software version 4.0 or later, and BlackBerry® Desktop Software version 4.0 or later support AES.

For more information about how the BlackBerry Enterprise Server uses AES for BlackBerry transport layer encryption to communicate with BlackBerry devices, visit www.blackberry.com/support to read article KB05429.

How a BlackBerry device uses the AES algorithm to help protect user data and keys

The BlackBerry® device implementation of the AES algorithm is designed to help protect user data and keys (such as the device transport key and ephemeral key) from traditional attacks and side-channel attacks.

A traditional attack tries to exploit data that a cryptographic system stores or transmits. The potentially malicious user tries to determine the key or the plain-text data by exploiting a weakness in the design of the cryptographic algorithm or protocol.

The potentially malicious user uses a side-channel attack to try to exploit the physical properties of the BlackBerry device implementation of the AES algorithm using power analysis (for example, SPA and DPA) and electromagnetic analysis (for example, SEMA and DEMA). A potentially malicious user tries to determine the keys that the BlackBerry device uses by measuring and analyzing the power consumption or the electromagnetic radiation that the BlackBerry device emits during cryptographic operations. The BlackBerry device uses a masking operation, table splitting, and a random mask application to help protect the keys and plain-text data against side-channel attacks at all points during the encryption and decryption operations.

Process flow: Running a masking operation during the first AES calculation when content protection is turned on

During the first AES calculation, the BlackBerry® device performs the following actions if you or a user turned on content protection:

1. runs a masking operation by performing the following actions:
   a. creates a mask table (*M*), where each table entry is a random value
   b. creates a masked version of the S-Box table (*S'*) that is used within AES
   c. periodically and randomly changes the order of all table entries
2. runs the result of step 1 as the input through both *M* and *S'*
3. combines the output of step 2 from *M* and *S'*
4. deletes the mask and produces the AES output

Process flow: Running a masking operation during subsequent AES calculations when content protection is turned on

A BlackBerry® device performs the following actions:

1. performs the masking operation by periodically and randomly permuting all table entries in every calculation
2. runs the input through both *M* and *S'*
3. combines the output from *M* and *S'*
4. deletes the mask and produces the AES output

Process flow: Running a masking operation when a BlackBerry device does not use content protection

If you or a user did not turn on content protection, aBlackBerry® device performs the following actions during an AES calculation:

1. masks the output from the round key
2. masks the AES S-Box input
3. masks the AES S-Box output

How the AES algorithm creates S-Box tables and uses round keys and masks

A BlackBerry® device permutes each AES S-Box entry at random and masks each entry with a random value.

The BlackBerry device masks the round keys with random values and any S-Box masks that the AES algorithm requires to work. Round keys are subkeys that the key schedule calculates for each round of encryption.

The BlackBerry device changes the random masks periodically and uses extra S-Box data to make identification of the S-Box table difficult, whether the BlackBerry device uses the S-Box table in the encryption process, decryption process, or key schedule process.

How the BlackBerry Enterprise Solution uses Triple DES to encrypt data

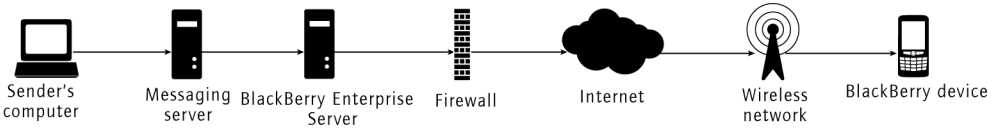
The BlackBerry® Enterprise Solution uses a two-key Triple DES encryption algorithm to generate message keys and device transport keys. In the three iterations of the DES algorithm, the first 56-bit key in outer CBC mode encrypts the data, the second 56-bit key decrypts the data, and the first key encrypts the data again.

The BlackBerry Enterprise Solution stores the message keys and device transport keys as 128-bit binary strings with each parity bit in the least significant bit of each of the 8 bytes of key data. The message keys and device transport keys have overall key lengths of 112 bits and include 16 bits of parity data.

All versions of the BlackBerry® Enterprise Server, BlackBerry® Device Software, and BlackBerry® Desktop Software support Triple DES.

For more information about Triple DES, see *Federal Information Processing Standard - FIPS PUB 81 [3]*.

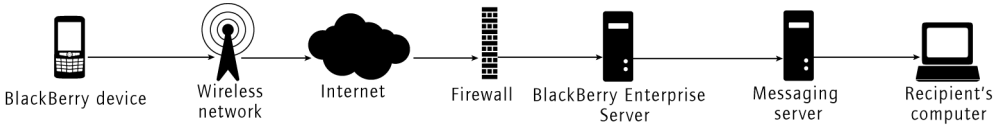
Process flow: Sending an email message to a BlackBerry device using BlackBerry transport layer encryption



1. A sender sends an email message to a BlackBerry® device user.
2. The BlackBerry® Enterprise Server performs the following actions:
   a. compresses the email message
   b. encrypts the email message using the message key
   c. encrypts the message key using the device transport key of the BlackBerry device
   d. sends the encrypted email message and encrypted message key to the BlackBerry device
3. The BlackBerry device user clicks on the email message on the BlackBerry device to open it.
4. The BlackBerry device performs the following actions:
   a. decrypts the message key using the device transport key

b. decrypts the email message using the message key
c. decompresses the email message
d. displays the email message to the user

Process flow: Sending an email message from a BlackBerry device using BlackBerry transport layer encryption



1. A sender sends an email message from a BlackBerry® device to a recipient.
2. The BlackBerry device performs the following actions:
   a. compresses the email message
   b. encrypts the compressed email message using the message key
   c. encrypts the message key using the device transport key of the BlackBerry device
   d. sends the encrypted message key and encrypted email message to the BlackBerry® Enterprise Server
3. The BlackBerry Enterprise Server performs the following actions:
   a. decrypts the message key using the device transport key
   b. decrypts the email message using the message key
   c. decompresses the email message
   d. forwards the email message to the recipient

Managing BlackBerry Enterprise Solution security 5

Using an IT policy to manage BlackBerry Enterprise Solution security

You can use an IT policy to control a BlackBerry® device, a BlackBerry enabled device, the BlackBerry® Desktop Software, and the BlackBerry® Web Desktop Manager in your organization's environment. An IT policy consists of multiple IT policy rules that manage the security and behavior of the BlackBerry® Enterprise Solution. For example, you can use IT policy rules to manage the following security features and behaviors of the BlackBerry device:

- encryption (for example, encryption of user data and messages that the BlackBerry® Enterprise Server forwards to message recipients) and encryption strength
- use of a password or pass phrase
- connections that use Bluetooth® wireless technology
- protection of user data and device transport keys on the BlackBerry device
- control of BlackBerry device resources, such as the camera or GPS, that are available to third-party applications

The BlackBerry Enterprise Server includes preconfigured IT policies that you can use to manage the security of the BlackBerry Enterprise Solution. The Default IT policy includes IT policy rules that are configured to indicate the default behavior of the BlackBerry device or BlackBerry Desktop Software.

After a BlackBerry device user activates a BlackBerry device, the BlackBerry Enterprise Server automatically sends to the BlackBerry device the IT policy that you assigned to the user account or group. By default, if you do not assign an IT policy to the user account or group, the BlackBerry Enterprise Server sends the Default IT policy. If you delete an IT policy that you assigned to the user account or group, the BlackBerry Enterprise Server automatically re-assigns the Default IT policy to the user account and resends the Default IT policy to the BlackBerry device.

For more information, see the *BlackBerry Enterprise Server Policy Reference Guide*.

Using IT policy rules to manage BlackBerry Enterprise Solution security

You can use IT policy rules to customize and control the actions that the BlackBerry® Enterprise Solution can perform.

To use an IT policy rule on a BlackBerry device, you must verify that the BlackBerry® Device Software version supports the IT policy rule. For example, you cannot use the Disable Camera IT policy rule to control whether a BlackBerry device user can access the camera on the BlackBerry device if the BlackBerry Device Software version does not support the IT policy rule. For information about the BlackBerry Device Software version that is required for a specific IT policy rule, see the *BlackBerry Enterprise Server Policy Reference Guide*.

The BlackBerry Administration Service groups the IT policy rules by common properties or by application. Most IT policy rules are designed so that you can assign them to multiple user accounts and groups.

Sending an IT policy over the wireless network

If your organization's environment includes C++ based BlackBerry® devices that are running BlackBerry® Device Software version 2.5 or later or Java® based BlackBerry devices that are running BlackBerry Device Software version 3.6 or later, the BlackBerry® Enterprise Server can send changes to IT policies to a BlackBerry device over the wireless network automatically. When the BlackBerry device receives an updated IT policy or a new IT policy, the BlackBerry device, BlackBerry® Desktop Software, and BlackBerry® Web Desktop Manager apply the configuration changes immediately.

By default, the BlackBerry Enterprise Server is designed to resend an IT policy to the BlackBerry device within a short period of time after you update the IT policy using the BlackBerry Administration Service. You can also resend an IT policy to a specific BlackBerry device manually. You can configure the BlackBerry Enterprise Server to resend the IT policy to the BlackBerry device at scheduled intervals regardless of whether you changed the IT policy.

Using IT administration commands to protect a lost or stolen BlackBerry device

The BlackBerry® Enterprise Server includes IT administration commands that you can send over the wireless network to protect sensitive data on a BlackBerry device. You can use these commands to lock the BlackBerry device, permanently delete user information and application data, and return the BlackBerry device settings to the default values.

IT administration command	Description
Specify new device password and lock device	This command creates a new password and locks a BlackBerry device over the wireless network. You can communicate the new password to the user verbally when the BlackBerry device user locates the BlackBerry device. When the BlackBerry device user unlocks the BlackBerry device, the BlackBerry device prompts the user to accept or reject the new password. You can use this command if the BlackBerry device is lost. If you or a user turned on content protection and a BlackBerry device is running BlackBerry® Device Software version 4.3.1 or earlier, you cannot use this command.
Delete all device data and disable device	This command permanently deletes all user information and application data that the BlackBerry device stores. You can configure the following options when you use this command: • specify a delay, in hours, before the BlackBerry device starts to delete all the user information and application data

IT administration command	Description
	• require the BlackBerry device to return to its factory default settings when it receives this command • specify whether to permit the BlackBerry device user to stop permanently deleting data from the BlackBerry device and making the BlackBerry device unavailable during the delay period You can send this command to a BlackBerry device that you want to distribute to another BlackBerry device user in your organization, or to a BlackBerry device that is lost and that the BlackBerry device user might recover.

Process flow: Sending the Specify new device password and lock device IT administration command when content protection is turned on

1. The BlackBerry® Enterprise Server sends the Specify new device password and lock device IT administration command and the new BlackBerry device password to the BlackBerry device.
2. The BlackBerry device performs the following actions:
   a. selects *r* randomly
   b. stores *r* in RAM
   c. calculates $D' = rD = rdP$
   d. calculates $h = SHA\text{-}1(B)$
   e. sends *D'* and *h* to the BlackBerry Enterprise Server
3. The BlackBerry Enterprise Server performs the following actions:
   a. uses *h* to determine which *B* the BlackBerry device used and which *b* to use
   b. verifies that *D'* is a valid public key
   c. calculates $K' = bD' = brdP = rdB = rK$ (the BlackBerry Enterprise Server knows only *rK* and cannot calculate *K* without *r*)
   d. calculates $h = SHA\text{-}1(D')$
   e. sends the new BlackBerry device password, *K'*, and *h* to the BlackBerry device
4. The BlackBerry device performs the following actions:
   a. uses *h* to verify that *K'* is associated with *D'* and *r*
   b. verifies that *K'* is a valid public key
   c. calculates $r^{-1}K' = r^{-1}rK = K$
   d. permanently deletes *r*

e. uses *K* to decrypt the content protection key
f. permanently deletes *K*

5. The BlackBerry device performs the following actions:
   a. selects *d* randomly
   b. calculates *D = dP*
   c. stores *D* in flash memory
   d. calculates *K = dB*
   e. uses *K* to encrypt the new BlackBerry device password
   f. uses the encrypted new password to encrypt the content protection key

Managing BlackBerry device access to the BlackBerry Enterprise Server

You can use the Enterprise Service Policy to control which BlackBerry® devices can connect to a BlackBerry® Enterprise Server. By default, after you turn on the Enterprise Service Policy, the BlackBerry Enterprise Server permits connections from any BlackBerry device or BlackBerry enabled device that you previously associated with the BlackBerry Enterprise Server. The BlackBerry Enterprise Server also prevents connections from any BlackBerry device that you associate with the BlackBerry Enterprise Server after you turn on the Enterprise Service Policy.

You can configure an allowed list to determine which BlackBerry devices can access a BlackBerry Enterprise Server. A BlackBerry device that meets the criteria that you specify in the allowed list can associate with the BlackBerry Enterprise Server when the BlackBerry device activates over the wireless network.

You can define the following types of criteria:

- specific BlackBerry device PINs
- range of BlackBerry device PINs
- specific manufacturers
- specific BlackBerry device models

The BlackBerry Administration Service includes lists of permitted manufacturers and models of BlackBerry devices that you associated with the BlackBerry Enterprise Server previously.

You can permit a user to override the Enterprise Service Policy so that a BlackBerry device or BlackBerry enabled device can connect to the BlackBerry Enterprise Server even if you configure the allowed list with criteria that exclude that BlackBerry device or BlackBerry enabled device.

For more information, see the *BlackBerry Enterprise Server Administration Guide*.

Using a segmented network architecture to prevent the spread of malware

To help prevent the spread of malware in your organization's network, you can use firewalls to divide your organization's network or LAN into segments and create a segmented network architecture. Each segment can manage the network traffic for a specific BlackBerry® Enterprise Solution component. A segmented network architecture is designed to improve the security and performance of a segment by filtering out data that is not destined for the segment.

To configure the BlackBerry Enterprise Solution in a segmented network architecture, you must install each BlackBerry Enterprise Solution component on a computer that is separate from the computers that host other components and then place each computer in its own network segment. When you configure the BlackBerry Enterprise Solution in a segmented network architecture, you create an architecture that is designed to prevent the spread of potential attacks from one computer that hosts a BlackBerry Enterprise Solution component to another computer within your organization's LAN. A segmented network architecture is designed to isolate and contain attacks on one computer. When you install each BlackBerry Enterprise Solution component in its own segment, you must permit communications with other components by opening only the port numbers that the BlackBerry Enterprise Solution components use.

For more information about the port numbers that the BlackBerry Enterprise Solution components use, see the *BlackBerry Enterprise Server Administration Guide*.

Moving a BlackBerry device to a BlackBerry Enterprise Server that uses a different BlackBerry Configuration Database

If you move a BlackBerry® device to a BlackBerry® Enterprise Server that uses a different BlackBerry Configuration Database without using the BlackBerry Enterprise Transporter, you or a user must permanently delete all user data and application data, the device transport key, and the IT policy public key from the BlackBerry device.

You or the user must reactivate the BlackBerry device to generate a new device transport key. The BlackBerry® Enterprise Server that you move the BlackBerry device to must generate an IT policy key pair and digitally sign and send the IT policy and the IT policy public key to the BlackBerry device before the BlackBerry device can communicate with the BlackBerry Enterprise Server.

The BlackBerry Configuration Database that you migrated the BlackBerry device to stores the BlackBerry Enterprise Server name, the device transport key, and the IT policy private key.

Best practice: Controlling which applications can use the GPS feature on a BlackBerry device

By default, if a third-party application or a preloaded BlackBerry® Application on a BlackBerry device supports the GPS feature, the application can use the GPS feature. For example, BlackBerry® Maps is a preloaded BlackBerry Application that uses the GPS feature to permit a user to locate a global position.

Best practice	Description
Control which application on the BlackBerry device can use the GPS feature.	Consider preventing a third-party application or preloaded BlackBerry Application from accessing the global position of the BlackBerry device. To apply this best practice, you can use one of the following methods: • To prevent the BlackBerry device from permitting all third-party applications and preloaded BlackBerry Applications from accessing the GPS feature, change the value of the Disable GPS IT policy rule to Yes. • To prevent a third-party application from using the GPS feature, change the value of the Is Access to the GPS API Allowed application control policy rule to Not Permitted. Assign the application control policy to the software configuration.
Control when the BlackBerry device reports its location to the BlackBerry® Enterprise Server.	By default, the BlackBerry device does not use the GPS feature to report its location to the BlackBerry Enterprise Server. If you change the value for the Enable Enterprise Location Tracking IT policy rule to Yes, consider configuring the interval after which a BlackBerry device reports its location to the BlackBerry Enterprise Server. To apply this best practice, you can use the Enterprise Location Tracking Interval IT policy rule. You can also use the Enterprise Location Tracking User Prompt Message IT policy rule to create a message that the BlackBerry device displays to notify the user that you turned on the ability of the BlackBerry device to report its location to the BlackBerry Enterprise Server.

BlackBerry device memory

6

The BlackBerry® device memory consists of various sections that store user data and sensitive information such as keys. Third-party applications on a BlackBerry device cannot write to or access the sections that store sensitive information.

Section	Description
flash memory	The flash memory is a file system that is internal to the BlackBerry device. The flash memory stores application data and user data. You cannot physically remove the flash memory from the BlackBerry device. Sections of flash memory can store files that a user downloads or saves.
on-board device memory	The on-board device memory stores files that a user saves on a BlackBerry device. The BlackBerry device uses and exposes the on-board device memory similar to the way that the BlackBerry device uses and exposes a media card. When you or a user permanently deletes all device data, the BlackBerry device deletes the files from the on-board device memory, except for the system memory partition, which includes sample pictures and sample tunes.
NV store	The NV store persists in flash memory, and only the operating system of the BlackBerry device can write to it. Third-party application code cannot write to the NV store.
media card	The media card stores files that a user saves using a BlackBerry device. You or a user can save, access, and encrypt files on the media card from the BlackBerry device. When you or a user permanently deletes device data, the BlackBerry device does not delete the files from the media card unless the BlackBerry device is running BlackBerry® Device Software version 5.0 or later.

Changing when a BlackBerry device cleans the BlackBerry device memory

By default, the memory cleaner application runs on a BlackBerry® device when the BlackBerry device is inactive for a specified period of time. You or a BlackBerry device user can change when the memory cleaner application runs when any the following conditions exist:

- The BlackBerry device user synchronizes the BlackBerry device with a computer.
- The BlackBerry device user locks the BlackBerry device.
- The BlackBerry device locks after it is inactive for a specified period of time.
- The BlackBerry device user changes the time or time zone on the BlackBerry device.

To change when the memory cleaner application runs, you can use IT policies or the BlackBerry device user can turn on or turn off the memory cleaner application in the Security options on the BlackBerry device.

You or the BlackBerry device user cannot turn off the memory cleaner application on the BlackBerry device if any of the following conditions exist:

- You or the BlackBerry device user turns on content protection on the BlackBerry device.
- An application uses the RIM® Cryptographic API to create a private key or symmetric key.
- An application that registers with the memory cleaner application requires that memory cleaning application be turned on.
- The BlackBerry device user installs the S/MIME Support Package for BlackBerry® smartphones on the BlackBerry device and a private key exists on the BlackBerry device.
- The BlackBerry device user installs the PGP® Support Package for BlackBerry® smartphones on the BlackBerry device and a private key exists on the BlackBerry device.

If you or the BlackBerry device user turns on the the memory cleaner application, Java® based garbage collection process uses the memory cleaner application automatically. The garbage collection process overwrites data that the BlackBerry device no longer uses.

For more information about the IT policy rules that you can use to change when the memory cleaner application runs, see the *BlackBerry Enterprise Server Policy Reference Guide*.

When a BlackBerry device overwrites data in the BlackBerry device memory

A BlackBerry® device continually runs the memory cleaner application during the Java® based garbage collection process to overwrite data in the BlackBerry device memory that the BlackBerry device no longer uses.

The BlackBerry device runs the garbage collection process when any of the following conditions exist:

- You or a BlackBerry device user turns on content protection for the BlackBerry device.
- An application uses the RIM® Cryptographic API to create a private key or symmetric key.
- A third-party application turns on the garbage collection process by registering with the memory cleaner application on the BlackBerry device. The memory cleaner application instructs applications to empty caches and to free the BlackBerry device memory that is associated with sensitive application data that the applications no longer use.
- A BlackBerry device user installs the S/MIME Support Package for BlackBerry® smartphones on the BlackBerry device.
- A BlackBerry device user installs the PGP® Support Package for BlackBerry® smartphones on the BlackBerry device.

When the BlackBerry device runs the garbage collection process, the garbage collection process overwrites the data that the BlackBerry device no longer uses with zeroes, periodically runs the memory cleaner application, and overwrites the memory that the memory cleaner application frees.

Deleting all device data from the BlackBerry device memory

A BlackBerry® device is designed to permanently delete the following data from the NV store, flash memory, and on-board device memory:

- all user data
- any references to your organization's PIN encryption key
- any references to the device transport key
- if applicable, authentication information (for example, the binding information of the smart card)
- IT policy public key
- if you are resetting the BlackBerry device to the factory default settings, any references to past hashes of the BlackBerry device password
- record of time elapsed since the BlackBerry device was last turned on
- if you are resetting the BlackBerry device to the factory default settings, stored IT policy
- If specified, all third-party applications and application data

If you or a user turns on content protection, the BlackBerry device uses a memory-scrubbing process to overwrite the flash memory on the BlackBerry device and the on-board BlackBerry device memory. The memory-scrubbing process complies with United States government requirements for deleting sensitive user data, including *US Department of Defense Directive 5220.22-M* and *NIST Special Publication 800-88*.

For BlackBerry® Device Software versions 5.0 and later, if you configure the Media Card Format on Device Wipe IT policy rule the BlackBerry device can also delete all user data from a media card. By default, the user can choose to delete third-party applications and the user data on the media card when the user permanently deletes all deivce data.

For more information, visit www.blackberry.com/go/serverdocs to read *Erasing File Systems on BlackBerry Devices Technical Overview*.

When a BlackBerry device deletes device data

The BlackBerry® device is designed to delete device data from the BlackBerry device memory when any of the following events occurs:

- The user clicks Wipe Device, Wipe Handheld, or Security Wipe in the security options on the BlackBerry device.
- The user types the BlackBerry device password incorrectly more times than the Set Maximum Password Attempts IT policy rule or the associated BlackBerry device option permits. The default value is ten attempts.
- The user runs the application loader tool and types the BlackBerry device password incorrectly more times than the Set Maximum Password Attempts IT policy rule permits.
- The user uses the application loader tool to delete all user data and application data on the BlackBerry device. The user can choose to not delete the BlackBerry device applications.
- You send the Delete all device data and disable device IT administration command to the BlackBerry device with or without a delay (in hours), to the BlackBerry device. The maximum delay is 168 hours (7 days).

- You click the Remove user data from current device option in the BlackBerry Administration Service after you connect the BlackBerry device to the BlackBerry Administration Service. This option deletes all data and applications from the BlackBerry device even if service books do not exist on the BlackBerry device.

Using IT policy rules to specify when a BlackBerry device must delete device data

You can configure the following IT policy rules to require that a BlackBerry® device that runs BlackBerry® Device Software version 4.5 or later automatically deletes device data after a specific time or during specific conditions.

IT policy rule	Description
Secure Wipe Delay After IT Policy Received	This rule specifies the length of time (in hours) that can elapse after receiving an IT policy update or an IT administration command that a BlackBerry device deletes all user data.
Secure Wipe Delay After Lock	This rule specifies the length of time (in hours) after a BlackBerry device locks that the device deletes all user data.
Secure Wipe if Low Battery	This rule specifies whether a BlackBerry device deletes all user data if the battery power level is too low.

For more information, see the *BlackBerry Enterprise Server Policy Reference Guide*.

Resetting a BlackBerry device to factory default settings

You can use the Reset to Factory Defaults on Wipe IT policy rule to require that a BlackBerry® device reset to the factory default settings when the BlackBerry device receives the Delete all device data and disable device IT administration command over the wireless network. When you change the value for the IT policy rule to Yes and send the IT administration command to the BlackBerry device, the BlackBerry device resets to the factory default settings and permanently deletes all device data. If the BlackBerry device is running BlackBerry® Device Software versions 5.0 and later, the BlackBerry device also deletes the IT policy and removes third-party applications.

If the BlackBerry device is running BlackBerry Device Software version 5.0 and later and you change the value for the IT policy rule to Yes, the BlackBerry device resets to factory default settings when you send the IT administration command, when a user permanently deletes BlackBerry device data, or when the user exceeds the maximum number of password attempts.

When the BlackBerry device resets to the factory default settings, the BlackBerry device overwrites the BlackBerry device memory. If you or a user turned on content protection, the BlackBerry device also scrubs the BlackBerry device memory. When the BlackBerry device scrubs the BlackBerry device memory, it deletes any residual unmapped data.

Process flow: Deleting all device data from a BlackBerry device

The following actions occur when you or a user delete all device data.

1. The BlackBerry® device adds a Device Under Attack flag to the NV store. If a user removes the battery or the battery power drops to zero before the process ends, when the user replaces the battery, the process continues because the Device Under Attack flag is still present.
2. The BlackBerry device deletes the IT policy public key from the NV store to remove its binding with the BlackBerry® Enterprise Server. The BlackBerry device can bind to another BlackBerry Enterprise Server at a later time. The BlackBerry device does not use the memory-scrubbing process to overwrite the IT policy public key because it is not a protected or hidden value.
3. If applicable, the BlackBerry device deletes authentication information (for example, the binding information for the smart card) from the NV store. The BlackBerry device can bind to another smart card at a later time.
4. The BlackBerry device turns off the wireless transceiver.
5. The BlackBerry device deletes data in the persistent store in flash memory, including references to the device transport key and the copy of the principal encryption key.
6. If applicable, the BlackBerry device formats the on-board device memory on the BlackBerry device.
7. The BlackBerry device overwrites the flash memory with zeroes.
8. The BlackBerry device deletes the BlackBerry device password from the NV store.
9. If you or a user turned on content protection, the memory-scrub process overwrites the file system of the BlackBerry device flash memory and on-board BlackBerry device memory. The memory-scrub process overwrites the BlackBerry device heap in RAM, changing the state of each bit four times.
10. If you or a user specified that the data on the media card must be deleted, the memory scrub process overwrites the media card.
11. The BlackBerry device deletes the Device Under Attack flag from the NV store.
12. The BlackBerry device restarts.

Scrubbing the memory of a BlackBerry device when deleting all BlackBerry device data

When you or a user deletes all BlackBerry® device data for a BlackBerry device when content protection is turned on, the BlackBerry device runs the memory scrub process to overwrite the BlackBerry device heap that is in RAM, the flash memory, and the files that a user saved on the BlackBerry device.

Scrubbing the BlackBerry device heap in RAM when deleting all BlackBerry device data

To overwrite the BlackBerry® device heap that is in RAM for a BlackBerry device when content protection is turned on, the BlackBerry device changes the state of each bit four times. The memory scrub process for a BlackBerry device performs the following actions:

1. writes 0x33 to each byte ($0011\ 0011_2$)
2. deletes all bytes to 0x00 ($0000\ 0000_2$)
3. writes 0xCC to each byte ($1100\ 1100_2$)
4. deletes all bytes to 0x00 ($0000\ 0000_2$)
5. writes 0x55 to each byte ($0101\ 0101_2$)
6. deletes all bytes to 0x00 ($0000\ 0000_2$)
7. writes 0xAA to each byte ($1010\ 1010_2$)

Scrubbing the flash memory on a BlackBerry device when deleting all BlackBerry device data

For a BlackBerry® device that is running BlackBerry® Device Software version 4.6 or later and that has content protection turned on, the memory scrub process overwrites the NAND flash memory by writing a single character before it deletes the data. The memory scrub process writes 0x00 to each byte ($0000\ 0000_2$). The memory scrub process deletes all blocks and changes all bytes to 0xFF ($1111\ 1111_2$).

For a BlackBerry device that is running a version of BlackBerry Device Software that is earlier than version 4.6 and that has content protection turned on, the memory scrub process overwrites the NOR flash memory by changing the state of each bit four times. The memory scrub process performs the following actions:

1. writes 0x33 to each byte ($0011\ 0011_2$)
2. deletes all bytes to 0xFF to each byte ($1111\ 1111_2$)
3. writes 0xCC to each byte ($0x1100\ 1100_2$)
4. deletes all bytes to 0xFF ($1111\ 1111_2$)
5. writes 0x55 to each byte ($0x0101\ 0101_2$)
6. deletes all bytes to 0xFF ($1111\ 1111_2$)
7. writes 0xAA to each byte ($0x1010\ 1010_2$)
8. deletes all bytes to 0xFF ($1111\ 1111_2$)

Scrubbing the user files on a BlackBerry device when deleting all BlackBerry device data

If a BlackBerry® device supports a partition of flash memory to store files that a user saved to the on-board device memory and you or a user turned on content protection, the memory scrub process overwrites that section of the BlackBerry device memory by writing a single character before the memory scrub process deletes the data. The memory scrub process performs the following actions:

1. writes 0x55 to each byte ($0101\ 0101_2$)
2. writes 0xAA to each byte ($1010\ 1010_2$)
3. deletes all blocks, and changes all bytes to 0xFF ($1111\ 1111_2$) or 0x00 ($0000\ 0000_2$)

Protecting data on a BlackBerry device

7

Encrypting user data on a locked BlackBerry device

If you or a BlackBerry® device user turns on content protection, you or the user can configure a locked BlackBerry device to encrypt stored user data and data that the locked BlackBerry device receives. When you or a user turns on content protection, a locked BlackBerry device is designed to use AES-256 encryption to encrypt stored data and an ECC public key to encrypt data that the locked BlackBerry device receives.

For example, the locked BlackBerry device uses content protection to encrypt the following items:

- subject, location, meeting organizer, attendees, and any notes in all appointments or meeting requests
- all contact information in the contact list except for the contact title and category
- subject, email addresses of intended recipients, message body, and attachments in all email messages
- title and information that is included in the body of a note for all memos
- subject and all information that is included in the body of tasks
- if you use software tokens, contents of the .sdtid file seed that is stored in flash memory
- all data that is associated with third-party applications that a user installs on the BlackBerry device
- in the BlackBerry® Browser, content that web sites or third-party applications push to the BlackBerry device, any web sites that the user saves on the BlackBerry device, and the browser cache
- all text that replaces the text automatically that the user types on the BlackBerry device

You can change the Content Protection of Contact List IT policy rule to Required to prevent the user from turning off content protection for the contact list on the BlackBerry device. If you change the Content Protection of Contact List IT policy rule to Required, the BlackBerry device does not permit call display and does not share contacts over a Bluetooth® connection when the BlackBerry device is locked.

Configuring the encryption of BlackBerry device data on a locked BlackBerry device

You can turn on content protection of BlackBerry® device data on a locked BlackBerry device using the Content Protection Strength IT policy rule. You can choose a strength level that corresponds to the ECC key strength that your organization requires.

A user can turn on content protection on the BlackBerry device, in the BlackBerry device options, in the security options. The user can change the content protection strength to the same level that you specify using the IT policy rule or to a higher level.

After you or a user configures content protection, a BlackBerry device uses the ECC private key to decrypt a message that it received when it was locked. The longer the ECC private key, the more time the BlackBerry device requires to decrypt messages. You must choose a strength level that optimizes the encryption strength or that optimizes the decryption process.

The BlackBerry device uses the BlackBerry device password to generate an ephemeral key that the BlackBerry device uses to encrypt the content protection key and the ECC private key. If you change the content protection strength to Stronger so that the BlackBerry device uses a 283-bit ECC private key, you can consider changing the Minimum Password Length IT policy rule to enforce a minimum password length of 12 characters for the BlackBerry device password. If you change the content protection strength to Strongest so that the BlackBerry device uses a 571-bit ECC private key, you can consider changing the Minimum Password Length IT policy rule to enforce a minimum password length of 21 characters for the BlackBerry device password. These password lengths maximize the encryption strength that the longer ECC private keys are designed to provide. A smaller password length produces a weaker ephemeral key.

Process flow: Encrypting user data on a locked BlackBerry device

When a BlackBerry® device locks for the first time after you or a user turns on content protection, the BlackBerry device performs the following actions:

1. uses the content protection key to automatically encrypt the bulk of its stored user data and application data
2. frees the BlackBerry device memory that is associated with the decrypted content protection key and the decrypted ECC private key that is stored in RAM
3. uses the ECC public key to encrypt data that it receives

Process flow: Decrypting user data on an unlocked BlackBerry device

1. A user types the correct BlackBerry® device password to unlock a BlackBerry device.
2. The BlackBerry device performs the following actions:
    a. uses the password to derive the ephemeral key
    b. uses the ephemeral key to decrypt the encrypted content protection key and ECC private key that are stored in flash memory
    c. stores the decrypted content protection key and ECC private key in RAM
    d. uses the decrypted content protection key to decrypt the user data when the user tries to access user data (for example, an email message) that the BlackBerry device received and encrypted while it was locked
    e. uses the decrypted ECC private key to decrypt the user data and access the ECC-encrypted items (for example, the message body, subject, or recipient) when the user tries to access user data that the BlackBerry device encrypted while it was locked

When the BlackBerry device opens ECC-128 encrypted items (usually less than 40 messages), the BlackBerry device uses the ECC private key to decrypt the ECC-encrypted items. The BlackBerry device re-encrypts the items with the content protection key the next time that the BlackBerry device locks. If the BlackBerry device does not complete the re-encryption process before the user unlocks the BlackBerry device, the BlackBerry device resumes re-encryption when it locks again.

Encrypting the device transport key on a locked BlackBerry device

If you turn on content protection for device transport keys, a BlackBerry® device uses the principal encryption key to encrypt the device transport keys that are stored in flash memory. The BlackBerry device encrypts the principal encryption key using the content protection key. When a locked BlackBerry device receives data that is encrypted using the device transport key, it uses the decrypted principal encryption key to decrypt the device transport key in flash memory and then uses the decrypted device transport key to decrypt data.

When you, a user, or a password timeout locks the BlackBerry device, the wireless transceiver remains on and the BlackBerry device does not delete the memory that is associated with the principal encryption key or device transport key. The BlackBerry device is designed to prevent the decrypted principal encryption key and the decrypted device transport key from appearing in flash memory.

You can turn on content protection for device transport keys on the BlackBerry device when you configure the Force Content Protection of Master Keys IT policy rule. When you turn on content protection of device transport keys, the BlackBerry device uses the ECC key strength that you specified in the Content Protection Strength IT policy rule to encrypt the device transport keys.

What happens when a user resets a BlackBerry device after you turn on content protection for the device transport key

If you turn on content protection of device transport keys, a BlackBerry® device performs the following actions when a user resets the BlackBerry device by removing and reinserting the battery:

- turns off the data connection over the wireless network
- suspends serial bypass connections if your organization's environment includes an enterprise Wi-Fi® network and the BlackBerry device can connect directly to a BlackBerry Router
- frees the memory that is associated with all data and keys, including the decrypted principal encryption key
- locks itself

The BlackBerry device is designed to turn off the data connection and serial bypass connection while the content protection key is unavailable to decrypt the principal encryption key in flash memory. Until a user unlocks the BlackBerry device, the BlackBerry device cannot receive and decrypt data. The BlackBerry device does not turn off the wireless transceiver and can still receive phone calls, SMS text messages, and MMS messages.

When the user unlocks the BlackBerry device after resetting it, the BlackBerry device performs the following actions:

- uses the content protection key to decrypt the principal encryption key in flash memory
- stores the decrypted principal encryption key in flash memory
- connects to the BlackBerry® Infrastructure
- resumes serial bypass connections
- receives data from the BlackBerry® Enterprise Server

Resetting a BlackBerry device password when content protection is turned on

If you or a user turns on content protection for a BlackBerry® device that is running BlackBerry® Device Software version 4.3 or later, you can reset the BlackBerry device password using a BlackBerry® Enterprise Server version 4.1 SP5 or later. The BlackBerry® Enterprise Solution uses the remote password reset cryptographic protocol to reset the BlackBerry device password when content protection is turned on. The BlackBerry device does not prompt the user for the old BlackBerry device password.

The remote password reset cryptographic protocol is designed to provide the following features:

- permit the BlackBerry device to encrypt the content protection key again with the new password, without the old password being available
- prevent a hardware-based attack on the BlackBerry device from recovering the content protection key without knowing either the BlackBerry device password or the IT policy private key that the BlackBerry Enterprise Server generates for the BlackBerry device
- prevent the BlackBerry Enterprise Server from accessing any data that a potentially malicious user could use to recover the content protection key

To reset the BlackBerry device password, you send the Specify new device password and lock device IT administration command to the BlackBerry device. You should send the IT administration command to a content-protected BlackBerry device that is in the possession of the BlackBerry device user only. If you send the IT administration command to a BlackBerry device that is in the possession of a potentially malicious user, that user can use a hardware-based attack to recover the key pair that the BlackBerry device created when it received the IT policy. The potentially malicious user can use the key pair to decrypt all the data on the BlackBerry device.

Process flow: Resetting a BlackBerry device password when content protection is turned on

The process flow is designed so that the BlackBerry® Enterprise Server cannot reconstruct the encryption key at a later time.

The BlackBerry Enterprise Server performs the following actions when you send the Specify new device password and lock device IT administration command to a BlackBerry device when content protection is turned on:

1. generates an encryption key using the IT policy public key and the NIST recommended 521-bit elliptic curve over a prime field
2. encrypts the content protection key using the encryption key and the new BlackBerry device password (which is also encrypted)
3. sends the data required to reconstruct the encryption key to the BlackBerry device

Cryptosystem parameters that the remote password reset cryptographic protocol uses

The BlackBerry® Enterprise Server and BlackBerry device are designed to share the following cryptosystem parameters when they use the remote password reset cryptographic protocol.

Uppercase parameters represent elliptic curve points. Lowercase parameters represent scalars. The elliptic curve group operations are additive.

Parameter	Description
E(Fq)	This parameter represents the NIST approved 521-bit random elliptic curve over *Fq*, which has a cofactor of 1.
Fq	This parameter represents a finite field of prime order q.
P	This parameter represents a point of E that generates a prime subgroup of *E(Fq)* of order p.
B = bP	This parameter represents the long-term IT policy public key and IT policy private key pair that the BlackBerry Enterprise Server generates for the BlackBerry device. The BlackBerry Enterprise Server stores *b* in the BlackBerry Configuration Database and sends *B* to the BlackBerry device in the IT policy.
D = dP	This parameter represents the key pair that the BlackBerry device creates when it receives *B*. The BlackBerry device stores *D*, but it deletes *d* to prevent a hardware-based attack from recovering *d* and *B* and then calculating *K = dB*.
K = dB	This parameter represents the encryption key that the BlackBerry device uses to encrypt the content protection key.
r	This parameter represents a short-term random number that the BlackBerry device stores in RAM.
D' = rD	This parameter represents a blinded version of *D*.
K' = bD' = brD = rK	This parameter represents a blinded version of *K*.

Protecting passwords that a BlackBerry device stores

A user can use the password keeper to store all passwords that the user uses to access applications and web sites from a BlackBerry® device. The password keeper is designed to protect the passwords with a password keeper password. The user is required to remember only the password keeper password.

The first time that the user opens the password keeper on the BlackBerry device, the user must create the password keeper password. The password keeper encrypts the information that it stores using AES-256 encryption, and uses the password keeper password to decrypt the information when the user types the password keeper password. The BlackBerry device deletes all device data if a user types the password keeper password incorrectly 10 times.

In the password keeper, a user can perform the following actions:

- type a password and its identifying information (for example, which application the user can access using the password), and save the information

- generate random passwords that are designed to improve password strength
- copy passwords and paste them into an application or password prompt for a web site

Protecting data that a BlackBerry device stores on a media card

To protect the data that a BlackBerry® device stores on a media card, you can configure the External File System Encryption Level IT policy rule, or a user can configure the corresponding option on the BlackBerry device. You can use this rule or option to configure whether the BlackBerry device encrypts the data using a password that a user provides, a BlackBerry device key that is randomly generated and stored in the NV store, or both.

A media card can store a master key and the code-signing keys that are included in the header information of encrypted files. The code-signing keys permit only applications that signed the files to access the files. A BlackBerry device is designed to use the master key that is stored on the media card to decrypt and encrypt files on the media card. The master key and code-signing keys use AES encryption. The BlackBerry device is designed to check the code-signing keys when the BlackBerry device opens the input streams or output streams of an encrypted file and to use code-signing with RSA-1024 encryption to control access to objects on the media card.

When a user stores a file on a media card for the first time after you or the user turns on encryption of media cards, the BlackBerry device decrypts the encryption key for the media card file and uses it to encrypt the stored file. The BlackBerry device does not encrypt files that a user transfers to the media card using a USB mass storage device.

The BlackBerry device, a computer, and other devices that use the media card can modify encrypted files (for example, truncate files) on the media card. The BlackBerry device is not designed to perform integrity checks on data in encrypted files.

For more information, visit www.blackberry.com/go/serverdocs to read *Enforcing Encryption of Internal and External File Systems on BlackBerry Devices Technical Overview*.

Process flow: Generating an encryption key for a media card

When you or a user turns on encryption of media cards for the first time, a BlackBerry® device generates an encryption key (also known as a session key) for a media card.

To generate an encryption key, the BlackBerry device performs the following actions:

1. generates an AES-256 encryption key
2. stores the encryption key in the NV store in RAM on the BlackBerry device
3. XORs the AES-256 encryption key with another AES-256 encryption key that is encrypted with a password to generate the encryption key for the media card
4. encrypts the encryption key for the media card using the AES-256 encryption key
5. stores the encrypted encryption key for media cards on the media card

How the BlackBerry Attachment Service protects data on a BlackBerry device

A BlackBerry® device uses the BlackBerry Attachment Service to process an attachment in an email message or calendar entry so that the user can view the attachment on the BlackBerry device. The BlackBerry Attachment Service is designed to prevent a potentially malicious application from accessing data on the BlackBerry device by using binary format parsing to open the attachment and process it.

After the BlackBerry Attachment Service processes the attachment, the BlackBerry Router sends the attachment to the BlackBerry device for rendering. If the attachment in the email message or calendar entry is an application, the BlackBerry device does not run the application.

For more information about the attachment file formats that the BlackBerry® Enterprise Server supports, see the *BlackBerry Enterprise Server Feature and Technical Overview*.

Best practice: Protecting the BlackBerry Attachment Service

To help prevent the spread of potential attacks from the computer that hosts the BlackBerry® Attachment Service to other computers in your organization's network, consider the following guidelines:

- Install the BlackBerry Attachment Service on a computer that is separate from the computer that hosts the BlackBerry® Enterprise Server.
- Place the computer that hosts the BlackBerry Attachment Service in its own network segment.

How a BlackBerry device protects its operating system and the BlackBerry Device Software

Each time a user turns on a BlackBerry® device, specific components on the BlackBerry device automatically check the authenticity of the BlackBerry device operating system and the integrity of the BlackBerry® Device Software. The BlackBerry Device Software must pass these security checks before the user can run the BlackBerry Device Software and before the user can update the BlackBerry Device Software over the wireless network.

How a BlackBerry device authenticates the boot ROM code and binds the BlackBerry device processor when the BlackBerry device turns on

A BlackBerry® device processor provides an authentication method that is designed to verify that the boot ROM code is permitted to run on a BlackBerry device. The manufacturing process installs the boot ROM code in flash memory on the BlackBerry device. The boot ROM code is the root of trust on BlackBerry devices. The RIM® signing authority system, which signs the boot ROM

code for a BlackBerry device during the manufacturing process, uses an RSA® public key to sign the boot ROM code. The processor is configured during the manufacturing process to store information that the processor can use to verify the digital signature of the boot ROM code.

When a user turns on a BlackBerry device, the processor runs internal ROM code that reads the boot ROM from flash memory and verifies the digital signature of the boot ROM code using the RSA public key. If the verification process is successful, the boot ROM is permitted to run on the BlackBerry device. If the verification process is not successful, the processor stops running.

The process of binding a processor to a boot ROM can occur when the processor is manufactured, the BlackBerry device is manufactured, or the BlackBerry® Device Software is configured, depending on the manufacturer and model number of the processor.

Protecting the data that the BlackBerry Enterprise Solution stores in your organization's environment 8

Where the BlackBerry Enterprise Server stores messages and user data in the messaging environment

The BlackBerry® Enterprise Server stores the messages and user data for a BlackBerry device in the messaging environment so that the BlackBerry Enterprise Server can maintain a connection between a user's email account and the BlackBerry device. To avoid compromising the user data that is stored in the messaging environment, you must protect the storage location in the messaging environment.

Messaging environment	Storage location
IBM® Lotus® Domino®	The following Lotus Domino databases store data for the BlackBerry Enterprise Server: • The BlackBerry state database stores an entry that opens a connection between each original email message in a user's IBM® Lotus Notes® Inbox and the same email message on the user's BlackBerry device. Each user account has a uniquely named BlackBerry state database. • The BlackBerry profiles database stores configuration information for each user account, including the identification information for the BlackBerry device and the device transport key. The BlackBerry profiles database stores a link to a BlackBerry state database and stores other information that the BlackBerry Enterprise Server uses to manage how email messages are sent to and from the BlackBerry device.
Microsoft® Exchange	The BlackBerry Enterprise Server stores user data in hidden folders in the Microsoft Exchange mailbox for the user.
Novell® GroupWise®	The BlackBerry Enterprise Server stores user data in the POA where the user account is located.

Data that the BlackBerry Configuration Database stores

The BlackBerry® Configuration Database stores the following information:

- name of each BlackBerry® Enterprise Server
- unique SRP authentication keys and unique SRP IDs, or UIDs, that each BlackBerry Enterprise Server uses in the SRP authentication process to open a connection to the wireless network
- IT policy private keys of the IT policy key pairs that the BlackBerry Enterprise Server generates for each BlackBerry device
- PIN of each BlackBerry device
- read-only copies of each device transport key
- copy of your organization's user directory
- a semi-permanent reference to user data using the Novell® GroupWise® MessageID in the database synchronization tables that are named MBMailSync, MBCalendarSync, MBPIMSync, and MBFolderSync (BlackBerry® Enterprise Server for Novell® GroupWise® only)

The BlackBerry Enterprise Server components that do not connect to a messaging server can access the information that the BlackBerry Configuration Database stores.

Best practice: Protecting the data that the BlackBerry Configuration Database stores

Best practice	Description
Audit connections to the Microsoft® SQL Server®.	Consider the following guidelines: • At a minimum, write failed connection attempts to the Microsoft SQL Server log file and review the log file regularly. • When possible, save log files to a different hard disk drive than the one that the data files are stored on.
Delete unsecured, old setup files.	Consider deleting Microsoft SQL Server setup files that might contain plaintext, credentials encrypted with weak public keys, or sensitive information that the Microsoft SQL Server logged to a Microsoft SQL Server version-dependent location during the Microsoft SQL Server installation process. Microsoft distributes the Killpwd tool, which is designed to locate and delete passwords from unsecured, old setup files in your organization's environment. For more information, visit support.microsoft.com to read article KB263968.
Limit the permission level of the Microsoft SQL Server.	Consider associating each Microsoft SQL Server service with a Windows® account that the service derives its security context from.

Best practice	Description
	Microsoft SQL Server permits the sa account and, in some cases, other user accounts to access operating system calls based on the security context of the account that runs the Microsoft SQL Server service. If you do not limit the permission level of the Microsoft SQL Server, a potentially malicious user might use these operating system calls to attack any other resource that the account has access to.
Make the Microsoft SQL Server port numbers that are monitored by default on your organization's firewall unavailable.	Consider configuring your organization's firewall to filter packets that are addressed to TCP port 1433, addressed to UDP port 1434, or associated with named instances.
Protect the sa account using a password.	Consider assigning a password to the sa account on the Microsoft SQL Server, even on servers that require Windows authentication. The password is designed to prevent an empty or weak password for the sa account from being exposed if an administrator of the database resets the Microsoft SQL Server for mixed mode authentication.
Protect the Microsoft SQL Server installation from Internet-based attacks.	Consider the following guidelines: • Require Windows Authentication Mode for connections to the Microsoft SQL Server to restrict connections to Windows user accounts and domain user accounts, and turn on credentials delegation. Windows Authentication Mode does not require you to store passwords on the computer. • Use stronger authentication protocols, required password complexity, and required expiration times.
Use a secure file system.	Consider the following guidelines: • Use NTFS for the Microsoft SQL Server because it is more stable and recoverable than FAT file systems, and NTFS permits security options such as file and directory ACLs and EFS. • Do not change the permissions that the Microsoft SQL Server specifies during the Microsoft SQL Server installation process. The Microsoft SQL Server creates appropriate ACLs on registry keys and files if it detects NTFS. • If you must change the account that runs the Microsoft SQL Server, decrypt the files that you could access using the old account and encrypt them again for access using the new account.
Use Microsoft SQL Server Management Studio.	Consider the following guidelines:

Best practice	Description
	• Use Microsoft SQL Server Management Studio to change the account that is associated with a Microsoft SQL Server service, if required. Microsoft SQL Server Management Studio configures the appropriate permissions on the files and registry keys that the Microsoft SQL Server uses. • Do not use the Microsoft Management Console Services applet to change the account that is associated with a Microsoft SQL Server service. To use this applet, you must manually change the Windows registry, the permissions for the NTFS file system, and Windows user rights. For more information, visit support.microsoft.com to read article KB283811.

How the BlackBerry Enterprise Solution protects IT policies

After the BlackBerry® Enterprise Server installation process creates the BlackBerry Configuration Database, the BlackBerry Enterprise Server generates an IT policy key pair that it can use to authenticate and protect the IT policy. When you assign a BlackBerry device to the user account and activate the BlackBerry device, the BlackBerry Enterprise Server sends the IT policy and the IT policy public key to the BlackBerry device.

The BlackBerry Enterprise Server stores the IT policy private key in the BlackBerry Configuration Database. The BlackBerry Enterprise Server uses the IT policy private key to digitally sign all data packets that include IT policy data when the BlackBerry Enterprise Server sends the IT policy to the BlackBerry device. The BlackBerry device uses the IT policy public key in the NV store to authenticate the digital signature on the IT policy.

A BlackBerry device stores the digitally signed IT policy and the IT policy public key in the NV store in flash memory. When the BlackBerry device stores the IT policy and IT policy public key, the BlackBerry device binds the IT policy to itself so that the BlackBerry device can use the IT policy to control its behavior.

Protecting communication with a BlackBerry device 9

Opening a direct connection between a BlackBerry device and a BlackBerry Router

A BlackBerry® Router and a BlackBerry device can use the BlackBerry Router protocol to bypass the SRP authenticated connection to the BlackBerry® Infrastructure and open a direct connection to each other. The BlackBerry Router can open a direct connection to a BlackBerry device that a user connects to a computer that hosts the BlackBerry® Device Manager. The BlackBerry Router can also open a direct connection to a BlackBerry device over an enterprise Wi-Fi® network using port 4101.

Before the BlackBerry® Enterprise Server or BlackBerry device send any data to each other, the BlackBerry device must authenticate with the BlackBerry Enterprise Server by verifying the device transport key. The BlackBerry Router opens an authenticated connection after the BlackBerry device authenticates with the BlackBerry Enterprise Server. The BlackBerry Router does not know the value of the device transport key that the BlackBerry Enterprise Server and BlackBerry device share.

If the BlackBerry device connects to the BlackBerry Router over the enterprise Wi-Fi network, after the BlackBerry Router opens an authenticated connection, the BlackBerry Router sends the Internet content requests or intranet content requests from the BlackBerry device to the enterprise Wi-Fi network over port 4101. The BlackBerry Router verifies that the PIN belongs to a BlackBerry device that is registered with the wireless network.

If you want the BlackBerry Router and BlackBerry device to use the BlackBerry Router protocol, you can consider installing the BlackBerry Router on a computer that is separate from the computer that hosts the BlackBerry Enterprise Server to prevent direct access to the computer that hosts the BlackBerry Enterprise Server.

Process flow: Authenticating a BlackBerry device with the BlackBerry Enterprise Server using the BlackBerry Router protocol

1. A user connects a BlackBerry® device to a computer that hosts the BlackBerry® Device Manager or connects a BlackBerry device to an enterprise Wi-Fi® network.
2. The BlackBerry® Enterprise Server and BlackBerry device use the BlackBerry Router protocol to verify that the BlackBerry device knows the device transport key.
   The BlackBerry Router protocol uses two runs of the elliptic curve version of the Schnorr identification scheme to provide mutual authentication between the BlackBerry Enterprise Server and BlackBerry device.
3. The BlackBerry Enterprise Server and BlackBerry device authenticate with each other using the same SRP authentication information that the BlackBerry Enterprise Server uses to authenticate with the BlackBerry® Infrastructure.
4. The BlackBerry Router opens an authenticated connection.

Closing a direct connection between a BlackBerry device and BlackBerry Router

If a user disconnects a BlackBerry® device from a computer that hosts the BlackBerry® Device Manager, closes the BlackBerry Device Manager, or disconnects the BlackBerry device from an enterprise Wi-Fi® network, the BlackBerry device restores the connection to the BlackBerry® Infrastructure over the wireless network automatically. The BlackBerry® Enterprise Server and BlackBerry Router use the BlackBerry Router protocol to close the authenticated connection to the BlackBerry device. The BlackBerry Router protocol is designed to permit only an authenticated party to close the connection. The BlackBerry Router uses a single execution of the Schnorr identification scheme to authenticate the close command that the BlackBerry Enterprise Server sends to the BlackBerry Router.

Impersonation attacks that the BlackBerry Router protocol is designed to prevent

The BlackBerry® Router protocol is designed to prevent a potentially malicious user from impersonating a BlackBerry device or a BlackBerry® Enterprise Server.

To impersonate the BlackBerry device, the potentially malicious user sends messages to the BlackBerry Enterprise Server so that the BlackBerry Enterprise Server believes it is communicating with the BlackBerry device. To impersonate the BlackBerry Enterprise Server, the potentially malicious user sends messages to the BlackBerry device so that the BlackBerry device believes it is communicating with the BlackBerry Enterprise Server.

To perform either of these impersonation attacks, the potentially malicious user must send the device transport key value (also known as *s*) to the BlackBerry Enterprise Server or BlackBerry device, which requires the potentially malicious user to solve the discrete log problem to determine *s* or the hash of *s*.

How the BlackBerry Router protocol uses the Schnorr identification scheme to open an authenticated connection

The implementation of the Schnorr identification scheme in the BlackBerry® Router protocol uses a group of large prime order, which is the additive group of elliptic curve points for a prime *p*.

The BlackBerry Router protocol is designed to perform the following actions:

- use the NIST recommended 521-bit elliptic curve group
- verify that the points supplied by the parties involved in the communication are members of the elliptic curve group
- verify that R_D does not equal R_B, to prevent the recovery of *h* by a potentially malicious user
- verify that *e* does not equal 0, to prevent the recovery of *h* by a potentially malicious user
- verify that R does not equal the point at infinity, to verify that R is a valid public key
- verify that *R* does not equal the point at infinity, to verify that *R* is a valid public key
- reset any corrupted data that it finds to a random value so that the BlackBerry Router protocol can proceed past the point that it detects corrupted data

Because the BlackBerry Router protocol can proceed past the point that it detects corrupted data, the BlackBerry Router protocol is unsuccessful at completion only. This measure is designed to prevent various timing attacks.

Process flow: Using the BlackBerry Router protocol to close an authenticated connection

1. The BlackBerry® Enterprise Server performs the following actions:
   a. selects a random value r_C, where $1 < r_c < p - 1$
   b. calculates $R_C = r_C P$
   c. calculates another R_C value if $R_C = R_B$, or $R_C = R_D$
   d. sends the value R_C to the BlackBerry Router
2. The BlackBerry Router performs the following actions:
   a. verifies that the value R_C is random when the value R_C approaches the point at infinity
   b. verifies that the value R_C is random when the value $R_C = R_B$, or $R_C = R_D$
   c. selects a random value e_C, where $1 < e_c < p - 1$
   d. calculates another e_C value if $e_C = e_D$, or $e_c = e_B$
   e. sends the value e_C to the BlackBerry Enterprise Server
3. The BlackBerry Enterprise Server performs the following actions:
   a. verifies that the value e_C is random when the value $e_C = 0$
   b. verifies that the value e_C is random when the value $e_C = e_B$, or $e_C = e_D$
   c. calculates $y_C = h - e_C r_C \bmod p$
   d. sends the value y_C to the BlackBerry Router
4. The BlackBerry Router performs one of the following actions:
   - The BlackBerry Router closes the authenticated connection to the BlackBerry device on behalf of the BlackBerry Enterprise Server if the BlackBerry Router accepts y_C.
   - The BlackBerry Router does not close the authenticated connection to the BlackBerry device if the BlackBerry Router calculates the following:

$$y_C P + e_C R_C \neq y_D P + e_D R_D$$

Process flow: Using the BlackBerry Router protocol to open an authenticated connection

1. The BlackBerry® device and BlackBerry® Enterprise Server hash the current device transport key using SHA-512.
2. The BlackBerry device performs the following actions:
   a. selects a random value r_D, where $1 < r_D < p - 1$ and calculates $R_D = r_D P$

b. sends R_D and a device transport key identifier (*KeyID*) to the BlackBerry Enterprise Server

3. The BlackBerry Router performs the following actions:
   a. observes the data that the BlackBerry device sends and verifies that the value R_D is not the point at infinity
   b. if R_D is the point at infinity, the BlackBerry Router configures R_D to a random value
   c. sends R_D and *KeyID* to the BlackBerry Enterprise Server
4. The BlackBerry Enterprise Server performs the following actions:
   a. calculates that as R_D approaches the point at infinity, R_D is random
   b. selects a random value r_B, where $1 < r_B < p - 1$ and calculates $R_B = r_B P$
   c. if $R_D = R_B$, calculates another value of R_B
   d. selects a random value e_D, where $1 < e_D < p - 1$
   e. sends R_B, e_D, and *KeyID* to the BlackBerry device
5. The BlackBerry Router performs the following actions:
   a. observes the data that the BlackBerry Enterprise Server sends
   b. verifies that the value R_B is random when the value R_B approaches the point at infinity or when $R_D = R_B$
   c. verifies that the value e_D is random when the value $e_D = 0$
   d. sends R_B, e_D, and *KeyID* to the BlackBerry device
6. The BlackBerry device performs the following actions:
   a. verifies that the value R_B is random when the value R_B approaches the point at infinity or when $R_D = R_B$
   b. verifies that the value e_D is random when the value $e_D = 0$
   c. calculates $y_D = h - e_D r_D \bmod p$
   d. selects a random value e_B, where $1 < e_B < p - 1$
   e. sends y_D and e_B to the BlackBerry Enterprise Server
7. The BlackBerry Router performs the following actions:
   a. observes the data that the BlackBerry device sends
   b. verifies that the value e_B is random if $e_B = 0$ or $e_B = e_D$
   c. forwards y_D and e_B to the BlackBerry Enterprise Server
8. The BlackBerry Enterprise Server performs the following actions:
   a. verifies that the value e_B is random when the value $e_D = e_B$
   b. verifies that the value e_D is random when the value $e_D = 0$
   c. computes $y_B = h - e_B r_B \pmod p$

d. sends y_B to the BlackBerry device

9. One of the following actions occurs:
   - The BlackBerry Enterprise Server and BlackBerry device open an authenticated connection to each other if the BlackBerry device accepts y_B.
   - The BlackBerry device does not accept the connection request, and the BlackBerry Enterprise Server and BlackBerry device do not open an authenticated connection to each other, if the BlackBerry device calculates the following:

     $$y_B P + e_B R_B \neq hP$$
   - The BlackBerry Router does not accept the connection request if the BlackBerry Router calculates the following:

     $$y_B P + e_B R_B \neq y_D P + e_D R_D$$
   - The BlackBerry Enterprise Server does not accept the connection request if the BlackBerry Enterprise Server calculates the following:

     $$y_D P + e_D R_D \neq hP$$
   - The BlackBerry Router stores R_D, R_B, $y_D P + e_D R_D$, e_D, and e_B if the BlackBerry device accepts y_B.
10. The BlackBerry Enterprise Server stores R_D, R_B, e_D, e_B, and h.
11. The BlackBerry Router overwrites y_B and y_D in memory with zeroes.
12. The BlackBerry Enterprise Server overwrites y_B, y_D, and r_B in memory with zeroes.
13. The BlackBerry device overwrites y_B, y_D, and r_D in memory with zeroes.

Cryptosystem parameters that the BlackBerry Router protocol uses

The BlackBerry® Router, BlackBerry® Enterprise Server, and BlackBerry device are designed to share the following cryptosystem parameters when they use the BlackBerry Router protocol.

Parameter	Description
E(Fq)	This parameter represents the NIST approved 521-bit random elliptic curve over *Fq*, which has a cofactor of 1. The BlackBerry Router protocol does all math operations in the groups *E(Fq)* and Z_p.
Fq	This parameter represents a finite field of prime order *q*.
P	This parameter represents a point of *E* that generates a prime subgroup of *E(Fq)* of order *p*.
xR	This parameter represents the elliptic curve scalar multiplication, where *x* is the scalar and *R* is a point on *E(Fq)*.
s	This parameter represents the value of the device transport key.
h	This parameter represents the SHA-512 hash of *s*.

Best practice: Protecting unsecured wireless messaging on the BlackBerry device

Unsecured wireless messaging includes SMS text messages, MMS messages, and PIN messages. A BlackBerry® device can send SMS text messages and MMS messages over a wireless TCP/IP connection.

Best practice	Description
Prevent a user from sending, forwarding, or replying to specific types of messages from the BlackBerry device.	Consider the following guidelines: • Prevent a user from forwarding or replying to a message using a BlackBerry® Enterprise Server that did not deliver the original message. • Prevent a user from using an email account to forward or reply to a PIN message or reply to an email message with a PIN message. To apply this best practice, you can use the Disable Forwarding Between Services IT policy rule.
Prevent external connections to a BlackBerry device.	Consider preventing applications on a BlackBerry device from opening external connections (for example, to WAP, SMS, MMS, or other public gateways). To apply this best practice, you can use the Allow External Connections IT policy rule.
Prevent plain-text PIN messages.	Consider preventing a user from sending plain-text PIN messages if your organization uses a highly secure messaging solution such as the S/MIME Support Package for BlackBerry® smartphones or the PGP® Support Package for BlackBerry® smartphones. To apply this best practice, you can use the Disable Peer-to-Peer Normal Send IT policy rule.
Prevent a BlackBerry device from using the global PIN encryption key.	Consider limiting the number of BlackBerry devices in your organization's environment that can receive SMS text messages, MMS messages, BlackBerry® Internet Service messages, PIN messages that use scrambling that is specific to your organization, and PIN messages that use the global PIN encryption key. To apply this best practice, you can use the Firewall Block Incoming Messages IT policy rule.

Best practice	Description
Require a user to verify whether the user wants to send a message.	Consider configuring the BlackBerry device so that the user must verify whether the user wants to send an email message, SMS text message, MMS message, or PIN message. To apply this best practice, you can use the Confirm on Send IT policy rule.
Turn off unsecured messaging on the BlackBerry device.	Consider turning off unsecured messaging to make sure that all communication for the BlackBerry device that starts in your organization travels through your organization's messaging environment. To turn off SMS text messaging, you can use the Allow SMS IT policy rule. To turn off MMS messaging, you can use the Disable MMS IT policy rule. To turn off PIN messaging, you can use the Allow Peer-to-Peer Messages IT policy rule. When you turn off PIN messaging, a user can receive PIN messages on the BlackBerry device but cannot send PIN messages from the BlackBerry device.

How the BlackBerry Enterprise Solution protects connections between a BlackBerry device and the Internet or intranet

A user can use the BlackBerry® Browser and BlackBerry Java® Applications on a BlackBerry device to access the Internet and your organization's intranet. The BlackBerry Browser and BlackBerry Java Applications can accept and respond to push requests from push applications. The BlackBerry Browser and BlackBerry Java Applications use the BlackBerry MDS Connection Service to access the Internet and your organization's intranet.

To access data on the Internet or your organization's intranet, the BlackBerry MDS Connection Service uses HTTP, TCP/IP, and the BlackBerry MDS security protocol. The BlackBerry MDS security protocol is a Research In Motion® proprietary protocol that is designed to protect messages that the BlackBerry device sends using the BlackBerry MDS Connection Service. The BlackBerry MDS Connection Service and BlackBerry device use BlackBerry transport layer encryption to help protect your organization's applications and the Internet data that a user receives on the BlackBerry device.

Authenticating data that a BlackBerry device sends to the BlackBerry MDS Integration Service

When a BlackBerry® device sends data to the BlackBerry MDS Integration Service, the BlackBerry MDS security protocol uses HMAC to authenticate part of each message header and message content, and to encrypt the MAC of each BlackBerry MDS message header. If necessary, the BlackBerry MDS security protocol also encrypts the content of each message.

The BlackBerry MDS security protocol uses a session key to authenticate data that the BlackBerry device sends to the BlackBerry MDS Integration Service. The BlackBerry device and BlackBerry MDS Integration Service share the same session key. The session key is stored in the BlackBerry Configuration Database. The BlackBerry MDS security protocol uses AES-128 in CBC mode with PKCS #5 padding to encrypt the session key using the database access key of the database server. The BlackBerry MDS security protocol also uses AES-128 in CBC mode with PKCS #5 padding to encrypt and decrypt data that the BlackBerry device and BlackBerry MDS Integration Service send between each other using the session key.

Using SSL to connect to web services

The BlackBerry® MDS Integration Service uses a certificate to permit client authentication between the BlackBerry MDS Integration Service and web services. By default, the BlackBerry MDS Integration Service generates a self-signed certificate when it starts after the BlackBerry MDS Integration Service installation process completes or when it cannot locate a certificate in the BlackBerry MDS Integration Service key store. You can replace the self-signed certificate with a signed certificate if the security policies in your organization require it.

If the BlackBerry MDS Integration Service must use SSL to connect to web services, you must export the certificate to the web services to authenticate communication with the web services. If a BlackBerry® MDS Runtime Application must use SSL to connect to web services, you can configure the BlackBerry® Enterprise Server to verify that the certificate chain for the certificate is strong enough. You can use the Weak Digest Algorithms IT policy rule to identify algorithms that the BlackBerry device and BlackBerry Enterprise Server should consider to be weak. After you configure authentication between the BlackBerry MDS Integration Service and web services, you can configure the BlackBerry device to install only BlackBerry MDS Runtime Applications that use SSL.

For more information, see the *BlackBerry Enterprise Server Administration Guide*.

Process flow: Registering a BlackBerry device with a BlackBerry MDS Integration Service

1. A BlackBerry® device performs the following actions:
   - generates an AES-128 session key
   - uses RSA-1024 with PKCS #1 padding to encrypt the AES session key
   - sends the AES-128 session key to the BlackBerry MDS Integration Service
   - stores the AES-128 session key in flash memory
2. The BlackBerry MDS security protocol on the BlackBerry MDS Integration Service uses AES-128 in CBC mode with PKCS #5 padding to encrypt a AES-128 session key using an AES-128 database access key.
3. The BlackBerry MDS Integration Service stores the encrypted AES-128 session key in the BlackBerry MDS Integration Service database and stores the AES-128 database access key in the database key store.
4. The BlackBerry MDS security protocol on the BlackBerry MDS Integration Service and BlackBerry device uses HMAC with a SHA-1 hash function and the 128-bit shared secret key to authenticate data that the BlackBerry device and BlackBerry MDS Integration Service send between each other.

The BlackBerry MDS security protocol uses AES-128 in CBC mode with PKCS #5 padding to encrypt and decrypt data that a BlackBerry device and BlackBerry MDS Integration Service send between each other.

How a BlackBerry device protects a connection to a WAP gateway

BlackBerry® Device Software versions 3.2 SP1 and later supports WTLS, which is designed to provide additional security when a BlackBerry device connects to a WAP gateway. A BlackBerry device can connect to a WAP gateway to access services that are provided by your organization's wireless service provider or to access a web site. WTLS encrypts and decrypts information, authenticates users, and provides data integrity.

For more information about WAP gateways, see your organization's wireless service provider.

Protecting HTTP connections from a BlackBerry device to content servers and application servers using HTTPS

If a third-party application on a BlackBerry® device can access servers on the Internet, you can configure the BlackBerry MDS Connection Service to use HTTPS to provide additional authentication and security for the connection. The BlackBerry device supports HTTPS in proxy mode using a proxy server or in direct mode using TLS.

If you configure HTTPS using a proxy server, the BlackBerry MDS Connection Service uses cipher suite components of Sun® JSSE version 1.4.1 to open the connection for the BlackBerry device. Typically, HTTP connections open faster using a proxy server than TLS.

If you configure HTTPS using TLS, the BlackBerry MDS Connection Service uses the TLS and WTLS key establishment algorithms, symmetric algorithms, and hash algorithms that the RIM® Cryptographic API supports to open the connection for the BlackBerry device. The BlackBerry device uses TLS to encrypt data that an application sends to content servers. The BlackBerry MDS Connection Service does not decrypt data that it sends over the wireless network. You can use TLS when only the end points of the transaction are trusted (for example, with banking services). A BlackBerry device that is running BlackBerry® Device Software version 3.6.1 or later supports TLS for connections.

What happens to data that is not delivered to a BlackBerry device

What happens to data that is not delivered because the connection between a BlackBerry Enterprise Server and the BlackBerry Infrastructure closes

Ten minutes after the connection between a BlackBerry® Enterprise Server and the BlackBerry® Infrastructure closes, the BlackBerry Infrastructure notifies the sender's BlackBerry device and deletes the message that is not delivered. The wireless network can queue up to 5 undelivered messages for up to 7 days. If more than 5 undelivered messages exist in the queue, the BlackBerry Enterprise Server stores the messages in the BlackBerry Configuration Database. The BlackBerry Infrastructure does not store data to send to BlackBerry devices.

If the BlackBerry Infrastructure is not responding and the connection closes unexpectedly, the wireless network deletes the undelivered messages. The BlackBerry device does not receive the messages and it does not send acknowledgment packets to the BlackBerry Enterprise Server. When the BlackBerry Infrastructure becomes available again, the BlackBerry Enterprise Server resends messages that it did not receive acknowledgment packets for.

What happens to data that is not delivered because a BlackBerry device is not available on the wireless network

When a user sends a message from a BlackBerry® device, the BlackBerry® Infrastructure might not be able to deliver the message to a BlackBerry device immediately if the BlackBerry device is not available on the wireless network. A BlackBerry device might not be available if it is outside a wireless coverage area or if the BlackBerry device is turned off.

If the BlackBerry Infrastructure cannot deliver a message after 10 minutes, the BlackBerry Infrastructure notifies the BlackBerry® Enterprise Server and deletes the message. The BlackBerry Enterprise Server requests a notification message from the BlackBerry Infrastructure when the BlackBerry device becomes available over the wireless network. When the BlackBerry device becomes available over the wireless network, the BlackBerry Infrastructure notifies the BlackBerry Enterprise Server. The BlackBerry Enterprise Server sends the message to the BlackBerry device.

If the message is not delivered after 7 days, the BlackBerry Infrastructure notifies the sender's BlackBerry device that it cannot deliver the message.

Protecting BlackBerry Enterprise Solution communications in your organization's environment

10

How a BlackBerry Enterprise Server and the BlackBerry Infrastructure authenticate with each other

The BlackBerry® Infrastructure and BlackBerry® Enterprise Server must authenticate with each other before they can transfer data. The BlackBerry Enterprise Server uses SRP to authenticate with and connect to the BlackBerry Infrastructure.

SRP is a point-to-point protocol that runs over TCP/IP. The BlackBerry Enterprise Server uses SRP to contact the BlackBerry Infrastructure and open a connection. When the BlackBerry Enterprise Server and BlackBerry Infrastructure open a connection, they perform the following actions:

- authenticate with each other
- exchange configuration information
- send and receive data

The BlackBerry Enterprise Server and BlackBerry Infrastructure use the SRP authentication key when they authenticate with each other. The SRP authentication key is a 20-byte encryption key that the BlackBerry Enterprise Server and BlackBerry Infrastructure share.

The BlackBerry Enterprise Server sends only outgoing traffic to a BlackBerry device using an authenticated connection to the BlackBerry Infrastructure.

What happens when a BlackBerry Enterprise Server and the BlackBerry Infrastructure open an initial connection

After a BlackBerry® Enterprise Server and the BlackBerry® Infrastructure open an initial connection over the Internet, the BlackBerry Enterprise Server is designed to send a basic information packet to the BlackBerry Infrastructure immediately. A basic information packet includes version information, SRP identifiers, and other information that is required to open an SRP connection. Both the BlackBerry Enterprise Server and BlackBerry Infrastructure can recognize the basic information packet. The BlackBerry Enterprise Server and BlackBerry Infrastructure can use the basic information packet to configure the parameters of the SRP implementation.

The BlackBerry Infrastructure does not send basic information packets to the BlackBerry Enterprise Server until after the BlackBerry Enterprise Server sends a packet to the BlackBerry Infrastructure. This process permits the BlackBerry Infrastructure to be backward compatible with previous BlackBerry Enterprise Server versions, which close the SRP connection if they receive unrecognized basic information packets.

How the BlackBerry Enterprise Solution protects a TCP/IP connection between a BlackBerry Enterprise Server and the BlackBerry Infrastructure

After a BlackBerry® Enterprise Server and the BlackBerry® Infrastructure open an SRP connection, the BlackBerry Enterprise Server uses a persistent TCP/IP connection to send data to the BlackBerry Infrastructure. The BlackBerry Infrastructure uses wireless network protocols (for example, GSM® or EDGE) to send data to the BlackBerry device. The TCP/IP connection between the BlackBerry Enterprise Server and BlackBerry Infrastructure is designed to be highly secure in the following ways:

- The BlackBerry Enterprise Server deletes data traffic that it receives from any source other than the messaging server, or from the BlackBerry device through the BlackBerry Infrastructure or BlackBerry® Desktop Software.
- The BlackBerry Enterprise Server and BlackBerry device use BlackBerry transport layer encryption to encrypt the data that they send to each other. No intermediate point decrypts and encrypts the data again.
- No data traffic of any kind can occur between the BlackBerry Enterprise Server and either the wireless network or the BlackBerry device unless the BlackBerry Enterprise Server can decrypt the data using a valid device transport key. Only the BlackBerry Enterprise Server and BlackBerry device have the correct device transport key.

You must configure your organization's firewall or proxy server to permit the BlackBerry Enterprise Server to start and maintain an outgoing connection to the BlackBerry Infrastructure over TCP port 3101.

Process flow: Authenticating a BlackBerry Enterprise Server with the BlackBerry Infrastructure

1. The BlackBerry® Enterprise Server sends a data packet that contains its unique SRP identifier to the BlackBerry® Infrastructure to claim the SRP identifier.
2. The BlackBerry Infrastructure sends a random challenge string to the BlackBerry Enterprise Server.
3. The BlackBerry Enterprise Server sends a challenge string to the BlackBerry Infrastructure.
4. The BlackBerry Infrastructure hashes the challenge string with the SRP authentication key using HMAC with the SHA-1 algorithm. The BlackBerry Infrastructure sends the resulting 20-byte value to the BlackBerry Enterprise Server as a challenge string.
5. The BlackBerry Enterprise Server hashes the challenge string with the SRP authentication key, and sends a challenge response to the BlackBerry Infrastructure.
6. The BlackBerry Infrastructure performs one of the following actions:
   - accepts the challenge response and sends a confirmation to the BlackBerry Enterprise Server to complete the authentication process and configure an authenticated SRP connection
   - rejects the challenge response

If the BlackBerry Infrastructure rejects the challenge response, the authentication process is not successful. The BlackBerry Infrastructure and BlackBerry Enterprise Server close the SRP connection. If a BlackBerry Enterprise Server uses the same SRP authentication key and SRP identifier to connect to (and then disconnect from) the BlackBerry Infrastructure 5 times in 1 minute, the BlackBerry Infrastructure deactivates the SRP identifier to help prevent a potentially malicious user from using the SRP identifier to create conditions for a DoS attack.

How a BlackBerry Enterprise Server and messaging server protect a connection to each other

A BlackBerry® Enterprise Server is designed to connect to the following messaging servers in a highly secure manner.

Messaging server	Description
IBM® Lotus® Domino®	The BlackBerry Enterprise Server and the Lotus Domino server communicate using the IBM® Lotus Notes® RPC protocol. A user who activates a BlackBerry device when the BlackBerry device is connected to a computer can encrypt data that is in transit between the Lotus Domino server and a Lotus Notes Inbox. For more information, see the online help for Lotus Domino.
Microsoft® Exchange	The BlackBerry Enterprise Server and Microsoft Exchange Server® communicate using the Microsoft Exchange Server RPC protocol. A user can use 128-bit encryption to encrypt RPC communication over the MAPI connection between the Microsoft Exchange server and Microsoft® Outlook®. For more information about turning on encryption, see the documentation for Microsoft Exchange.
Novell® GroupWise®	The BlackBerry Enterprise Server is designed to use a trusted application key to open a connection to the Novell GroupWise server. To generate the trusted application key, an administrator of Novell GroupWise runs the trusted application key generator, specifies the location of the primary domain of Novell GroupWise, and specifies the application name that the BlackBerry Enterprise Server can use to connect to the Novell GroupWise server. The trusted application key is a 64-byte ASCII string.

Messaging server	Description
	The BlackBerry Enterprise Server connects to a user's mailbox in a highly secure manner using the trusted application key. The Novell GroupWise server verifies the trusted application key and permits the BlackBerry Enterprise Server to open a connection to the Novell GroupWise database for the user.

How the BlackBerry Enterprise Server components and the BlackBerry MVS protect communication

BlackBerry® Enterprise Server components and the BlackBerry® Mobile Voice System use the BlackBerry inter-process protocol to help protect the data that the components send to each other. The BlackBerry inter-process protocol uses a communication password to generate a session key that encrypts the data that the components send to each other. The BlackBerry Collaboration Service, BlackBerry MDS Connection Service, BlackBerry Policy Service, BlackBerry Synchronization Service, and BlackBerry MVS share a communication password. The BlackBerry Messaging Agent and BlackBerry Dispatcher share a different communication password. The communication passwords are designed to prevent a potentially malicious user from viewing data that the the BlackBerry Enterprise Server components and the BlackBerry MVS send to each other.

When a BlackBerry Enterprise Server component or the BlackBerry MVS opens a connection to the BlackBerry Dispatcher, the BlackBerry inter-process protocol is designed to use SPEKE to generate the session key. The key generation process uses the communication password of the BlackBerry Enterprise Server component or BlackBerry MVS and generates an AES-256 encryption key, which is the session key. The BlackBerry Enterprise Server components and BlackBerry MVS use the session key to encrypt the data that the BlackBerry Enterprise Server components and BlackBerry MVS sends to other BlackBerry Enterprise Server components that share the same communication password.

How the BlackBerry Desktop Manager protects communication using the BlackBerry inter-process protocol

The application loader tool of the BlackBerry® Desktop Manager or the Roxio® Media Manager for BlackBerry® smartphones can prompt BlackBerry Desktop Manager version 4.2 or later for the BlackBerry device password.

To protect the BlackBerry device password, when the application loader tool or Roxio Media Manager for BlackBerry smartphones connects to the BlackBerry Desktop Manager, the BlackBerry Desktop Manager uses the BlackBerry inter-process protocol.

The application loader tool and Roxio Media Manager for BlackBerry smartphones share a communication password with the BlackBerry Desktop Manager. The BlackBerry inter-process protocol is designed to use the communication password to protect any communication between the BlackBerry Desktop Manager and the application loader tool or Roxio Media Manager for BlackBerry smartphones.

Process flow: Authenticating the application loader tool or Roxio Media Manager with the BlackBerry Desktop Software using the BlackBerry inter-process protocol

1. The application loader tool of the BlackBerry® Desktop Software or Roxio® Media Manager opens a connection to BlackBerry Desktop Software version 4.2 or later.
2. The BlackBerry Desktop Software implementation of the BlackBerry inter-process protocol performs the following actions:
   a. uses a shared secret password (also known as the secure communication password) and the ECDH protocol with a 521-bit curve to create a device transport key
   b. uses the device transport key to create two encryption keys and two HMAC-SHA-256 keys
   c. uses one encryption key and one HMAC key to encrypt and authenticate data that BlackBerry Desktop Software version 4.2 or later sends over the communication channel to the BlackBerry® Enterprise Solution components that share the secure communication password

The BlackBerry inter-process protocol uses one encryption key and one HMAC key to encrypt and authenticate data that BlackBerry Desktop Software version 4.2 receives over the communication channel from the application loader tool or Roxio Media Manager.

How the BlackBerry Collaboration Service protects the connections between the BlackBerry Collaboration Service and instant messaging server

The BlackBerry® Collaboration Service is designed to connect to an instant messaging server and the collaboration clients on BlackBerry devices. If your organization's instant messaging server is Microsoft® Office Live Communications Server 2005 or Microsoft® Office Communications Server 2007, the BlackBerry Collaboration Service connects to the Microsoft® Office Communicator Web Access server using HTTPS or HTTP.

Activating a BlackBerry device

11

When a user activates a BlackBerry® device, the BlackBerry® Enterprise Solution authenticates the user and associates the BlackBerry device with a BlackBerry® Enterprise Server. During the activation process, the BlackBerry Enterprise Solution generates a device transport key.

A user can activate the BlackBerry device over the wireless network, when the BlackBerry device is connected to a computer that is running the BlackBerry® Desktop Software, or when the BlackBerry device is connected to a computer and the user is logged in to the BlackBerry® Web Desktop Manager or BlackBerry Administration Service. The user must have a valid email address so that the user can activate the BlackBerry device and register the BlackBerry device with the wireless network.

Activating a BlackBerry device over the wireless network

If a user activates a BlackBerry® device over the wireless network, the user must authenticate with the BlackBerry device using an activation password that you provide. You can create an activation password using the BlackBerry Administration Service and communicate it to the user. You can also use IT policy rules to configure password requirements (such as duration, length, and strength), to specify password patterns, and to prevent specific passwords. For more information, see the *BlackBerry Enterprise Server Policy Reference Guide*.

The BlackBerry device uses the activation password to generate the device transport key. The device transport key authenticates the user and is designed to secure communication between the BlackBerry® Enterprise Server and BlackBerry device.

An activation password has the following characteristics:

- applies to the user's email account
- is not valid after five unsuccessful attempts to activate the BlackBerry device
- expires if the user does not activate the BlackBerry device within the default period of time (48 hours), or a period of up to 720 hours that you can specify when you create the activation password

After the user activates the BlackBerry device, the BlackBerry Enterprise Server deletes the activation password. The user cannot use the same activation password to activate other BlackBerry devices.

Process flow: Activating a BlackBerry device over the wireless network

1. A user opens the activation application on the BlackBerry® device, and types the appropriate email address and activation password.
2. The BlackBerry device sends an activation request to the BlackBerry® Infrastructure using standard BlackBerry protocols. The BlackBerry Infrastructure uses SMTP to send an activation message to the user's email account. The activation message contains routing information for the BlackBerry device and public keys.
3. The BlackBerry® Enterprise Server sends an activation response to the BlackBerry device. The activation response contains routing information for the BlackBerry Enterprise Server and the long-term public keys of the BlackBerry Enterprise Server.

4. The BlackBerry Enterprise Server and BlackBerry device use the initial key establishment protocol to generate a device transport key and verify it. If the BlackBerry Enterprise Server and BlackBerry device mutually verify the device transport key, the activation process proceeds. The BlackBerry Enterprise Server and BlackBerry device use the device transport key to encrypt further communication between each other without sending the device transport key over the wireless network.
5. The BlackBerry Enterprise Server performs the following actions:
   - sends the appropriate service books to the BlackBerry device so that the user can send messages from and receive messages on the BlackBerry device
   - sends data (such as calendar entries, contacts, tasks, memos, and BlackBerry device options) to the BlackBerry device, if you turn on wireless organizer data synchronization and wireless backup

For more information about the activation process, see the *BlackBerry Wireless Enterprise Activation Technical Overview*.

Enrolling certificates on a BlackBerry device over the wireless network

12

You can configure the BlackBerry® Enterprise Server to permit a BlackBerry device to enroll certificates over the wireless network. You can permit the BlackBerry device to enroll certificates over the wireless network so that you do not have to instruct the user to send the certificates in an email message or to use the certificate synchronization tool in the BlackBerry® Desktop Manager.

You can enroll certificates from one of the following certification authorities:

- RSA® certification authority
- Microsoft® standalone certification authority
- Microsoft enterprise certification authority

For more information about configuring the BlackBerry Enterprise Server to permit the BlackBerry device to enroll certificates over the wireless network, see the *BlackBerry Enterprise Server Administration Guide*.

Process flow: Enrolling a certificate when the certification authority approves certificate requests automatically

After a BlackBerry® device receives an IT policy that includes a certification authority profile, the enrollment process can start automatically, or you can instruct a user to start it. This process flow assumes that the certification authority in your organization's environment is a Microsoft® enterprise certification authority.

1. The CA Profile Manager on the BlackBerry device generates the key pair for the certificate.
2. The BlackBerry MDS Connection Service authenticates the user.
3. The BlackBerry device requests the user's distinguished name from the BlackBerry® Enterprise Server.
4. The BlackBerry Enterprise Server retrieves the user's distinguished name from the messaging server and sends the distinguished name to the BlackBerry device.
5. The BlackBerry device encrypts the key pair, and stores the key pair, distinguished name, and profile ID for the certification authority in the persistent store in flash memory.
6. The CA Profile Manager creates the PKCS #10 certificate request, and signs it with the private key.
7. The BlackBerry device sends the certificate request, profile ID for the certification authority, and Windows® login information to the BlackBerry MDS Connection Service.
8. The BlackBerry MDS Connection Service performs one of the following actions:
   - sends the certificate chain to the BlackBerry Enterprise Server if the certificate chain is in the BlackBerry MDS Connection Service cache
   - retrieves the certificate chain from the certification authority and sends it to the BlackBerry Enterprise Server if the certificate chain is not in the BlackBerry MDS Connection Service cache

9. The BlackBerry Enterprise Server sends the certificate chain to the BlackBerry device.
10. The BlackBerry MDS Connection Service sends a status update to the BlackBerry device and sends the certificate request to the certification authority that is associated with the profile ID.
11. The certification authority issues the certificate, publishes it to the LDAP server, and notifies the BlackBerry MDS Connection Service that the certificate is available.
12. The BlackBerry MDS Connection Service performs the following actions:
    a. retrieves the certificate from the LDAP server that the certification authority publishes the certificate to
    b. sends the certificate to the BlackBerry Enterprise Server
13. The BlackBerry Enterprise Server performs the following actions:
    a. verifies the certificate by checking whether the public key matches the public key that is stored in the BlackBerry Configuration Database
    b. sends the certificate to the BlackBerry device over the wireless network
14. The BlackBerry device adds the certificate and private key to the key store.

Process flow: Enrolling a certificate when a certification authority administrator approves certificate requests

After a BlackBerry® device receives an IT policy that includes a certification authority profile, the enrollment process can start automatically or you can instruct a user to start it. This process flow assumes that the certification authority in your organization's environment is a Microsoft® enterprise certification authority.

1. The CA Profile Manager on the BlackBerry device generates the key pair for the certificate.
2. The BlackBerry MDS Connection Service authenticates the user.
3. The BlackBerry device requests the user's distinguished name from the BlackBerry® Enterprise Server.
4. The BlackBerry Enterprise Server retrieves the user's distinguished name from the messaging server and sends the distinguished name to the BlackBerry device.
5. The BlackBerry device encrypts the key pair, and stores the key pair, distinguished name, and profile ID for the certification authority in the persistent store in flash memory.
6. The CA Profile Manager creates the PKCS #10 certificate request and signs it with the private key.
7. The BlackBerry device sends the certificate request, profile ID for the certification authority, and Windows® login information to the BlackBerry MDS Connection Service.
8. The BlackBerry MDS Connection Service performs one of the following actions:
    - sends the certificate chain to the BlackBerry Enterprise Server if the certificate chain is in the BlackBerry MDS Connection Service cache
    - retrieves the certificate chain from the certification authority and sends it to the BlackBerry Enterprise Server if the certificate chain is not in the BlackBerry MDS Connection Service cache

9. The BlackBerry Enterprise Server sends the certificate chain to the BlackBerry device.
10. The BlackBerry MDS Connection Service sends a status update to the BlackBerry device and sends the certification request to the certification authority that is associated with the profile ID.
11. The certification authority performs the following actions:
    a. waits for the certification authority administrator to approve the certificate request
    b. after the certification authority administrator approves the certificate request, issues the certificate, and sends the certificate to the user in an email message
12. The BlackBerry MDS Connection Service performs the following actions:
    a. polls the user's mailbox on the messaging server, at specified intervals, for the certificate
    b. sends the certificate to the BlackBerry Enterprise Server after the BlackBerry MDS Connection Service retrieves the certificate
13. The BlackBerry Enterprise Server performs the following actions:
    a. verifies the certificate by checking whether the public key matches the public key that is stored in the BlackBerry Configuration Database
    b. sends the certificate to the BlackBerry device over the wireless network
14. The BlackBerry device adds the certificate and private key to the key store.

Process flow: Enrolling a certificate using an RSA certification authority

After a BlackBerry® device receives an IT policy that includes a certification authority profile, the enrollment process can start automatically or you can instruct a user to start it.

1. The CA Profile Manager on the BlackBerry device generates the key pair for the certificate.
2. The BlackBerry device requests the user's distinguished name from the BlackBerry® Enterprise Server.
3. The BlackBerry Enterprise Server retrieves the user's distinguished name from the messaging server and sends the distinguished name to the BlackBerry device.
4. The BlackBerry device encrypts the key pair, and stores the key pair, distinguished name, and profile ID for the certification authority in the persistent store in flash memory.
5. The CA Profile Manager creates the PKCS #10 certificate request and signs it with the private key.
6. The BlackBerry device sends the certificate request and the name of the certification authority profile to the BlackBerry MDS Connection Service.
7. The BlackBerry MDS Connection Service performs one of the following actions:
    - sends the certificate chain to the BlackBerry Enterprise Server if the certificate chain is in the BlackBerry MDS Connection Service cache
    - retrieves the certificate chain from the certification authority and sends it to the BlackBerry Enterprise Server if the certificate chain is not in the BlackBerry MDS Connection Service cache

8. The BlackBerry Enterprise Server sends the certificate chain to the BlackBerry device.
9. The BlackBerry MDS Connection Service sends a status update to the BlackBerry device and sends the certificate request to the certification authority that is associated with the name of the certification authority profile.
10. The certification authority performs the following actions:
    a. waits for the certification authority administrator to approve the certificate request
    b. after the certification authority administrator approves the certificate request, issues the certificate, and sends the URL for the certificate in an email message to the user
11. The BlackBerry Messaging Agent receives the email message and extracts the issue ID of the message from the URL and stores it in the BlackBerry Configuration Database.
12. The BlackBerry MDS Connection Service performs the following actions:
    a. polls the BlackBerry Configuration Database every 5 minutes for the issue ID of the message, reconstructs the URL, and sends the URL to the certification authority to retrieve the certificate
    b. sends the certificate to the BlackBerry Enterprise Server after retrieving the certificate
13. The BlackBerry Enterprise Server perfoms the following actions:
    a. verifies the certificate by checking whether the public key matches the public key that is stored in the BlackBerry Configuration Database
    b. sends the certificate to the BlackBerry device over the wireless network
14. The BlackBerry device adds the certificate and private key to the key store.

Protecting BlackBerry Device Software updates 13

Protecting BlackBerry Device Software updates over the wireless network

You can update the BlackBerry® Device Software on a BlackBerry device over the wireless network. You can use the BlackBerry Administration Service to search for updates that match the BlackBerry device and wireless service provider, and send the updates. You can also permit your organization's wireless service provider to send the BlackBerry Device Software updates.

The BlackBerry® Enterprise Solution protects the BlackBerry Device Software updates using encryption, IT policies, content protection, and battery power requirements.

For more information about BlackBerry Device Software updates, see the *BlackBerry Device Software Update Guide*.

How the BlackBerry Enterprise Solution protects BlackBerry Device Software updates over the wireless network using encryption

The BlackBerry® Enterprise Server, BlackBerry® Infrastructure, BlackBerry® Provisioning System administration web site, and BlackBerry device protect data for BlackBerry® Device Software updates over the wireless network. You can use the BlackBerry Provisioning System administration web site when you want to permit your organization's wireless service provider to update the BlackBerry Device Software.

The BlackBerry Enterprise Server and BlackBerry device encrypt all data that they send between each other, including BlackBerry Device Software updates, using BlackBerry transport layer encryption.

The BlackBerry device validates the digital signatures of the following information to verify integrity:

- control messages that the BlackBerry device receives from the BlackBerry Infrastructure or BlackBerry Provisioning System administration web site
- BlackBerry Device Software update instructions that the BlackBerry device requests and receives from the BlackBerry Infrastructure or BlackBerry Provisioning System administration web site

How the BlackBerry Enterprise Solution protects BlackBerry Device Software updates over the wireless network using IT policies and content protection

The default values for the Default IT policy determine that only the BlackBerry® Enterprise Server can send available BlackBerry® Device Software updates and request a BlackBerry device to update the BlackBerry Device Software. A wireless service provider cannot send available BlackBerry Device Software updates to the BlackBerry device unless you change the value for the Allow Non Enterprise Upgrade IT policy rule to Yes.

When you or a user turns on the content protection feature on a BlackBerry device, the BlackBerry device protects user data in the following ways:

- requires the user to type the BlackBerry device password before the BlackBerry Device Software update process can back up or restore user data
- requires the BlackBerry device to encrypt stored user data during the BlackBerry Device Software update process

Battery power requirements for BlackBerry Device Software updates over the wireless network

The battery power level on a BlackBerry® device must be 50% or greater for the BlackBerry device to retrieve an update package over the wireless network. If the battery power level is below the minimum requirement, the update process suspends. The BlackBerry device prompts the user to recharge the battery and start the update process again. If the battery power level returns to 50%, the BlackBerry device resumes retrieving the update package from the BlackBerry® Infrastructure.

The battery power requirement is designed to protect the BlackBerry device against attacks from a potentially malicious user who might try to take advantage of low battery power during a BlackBerry Device Software update.

Process flow: Preparing to send a BlackBerry Device Software update over the wireless network

Before the BlackBerry® Infrastructure sends a BlackBerry® Device Software update to a BlackBerry device, the BlackBerry Infrastructure performs the following actions:

1. generates an ECDSA key periodically using ECC over a 521-bit curve
2. signs the ECDSA key using a stored root certificate
3. signs the BlackBerry Device Software update that it sends to the BlackBerry device using the digitally signed ECDSA key

How a BlackBerry device validates a BlackBerry Device Software update over the wireless network

When a BlackBerry® device receives a BlackBerry® Device Software update from the BlackBerry® Infrastructure, it verifies that the ECDSA key uses a public key that is shared by all BlackBerry devices that support BlackBerry Device Software updates over the wireless network. The BlackBerry device verifies the digital signature on the ECDSA key using a stored root certificate.

Updating the BlackBerry Device Software from an update web site

You can configure the IT policy rules that are included in the Wired Software Updates policy group to permit a user to update the BlackBerry® Device Software from an update web site using the BlackBerry® Desktop Manager or BlackBerry Application Web Loader. The user can use the update process to update the BlackBerry Device Software from a computer that is outside your organization's network (for example, from home).

During the update process, a BlackBerry device activates itself automatically over the wireless network so that the user can use a computer that is outside your organization's network to update the BlackBerry Device Software. When a user who does not use the BlackBerry Desktop Manager visits the update web site, the user must download and install Microsoft® ActiveX® components on the computer before the user can update the BlackBerry Device Software. The update process can take from 15 minutes to 2 hours, depending on the type of update, amount of BlackBerry device data, and number of applications that are installed on the BlackBerry device. A user cannot use the BlackBerry device or make emergency calls during the update process.

BlackBerry Device Software versions 5.0 and later, BlackBerry Desktop Manager versions 5.0.1 and later, and BlackBerry Application Web Loader versions 1.1.0 and later support BlackBerry Device Software updates from an update web site.

For more information about the IT policy rules that are included in the Wired Software Updates policy group, see the *BlackBerry Enterprise Server Policy Reference Guide*. For more information about the BlackBerry Application Web Loader, see the *BlackBerry Application Web Loader Developer Guide*.

Protecting cryptographic services data when updating the BlackBerry Device Software from an update web site

When a user updates the BlackBerry® Device Software from an update web site, the BlackBerry® Enterprise Solution backs up cryptographic services data (for example, cryptographic keys and service books) from a BlackBerry device to the user's computer. To protect the cryptographic services data, the BlackBerry device encrypts the cryptographic services data using a BlackBerry services key.

The BlackBerry device stores the BlackBerry services key in the NV store in flash memory. Neither the user nor third-party applications can access the location in the NV store where the BlackBerry device stores the BlackBerry services key. If you or a user turns on content protection, the BlackBerry device also encrypts the BlackBerry services key using the content protection key.

After the BlackBerry device encrypts the cryptographic services data, the BlackBerry® Desktop Manager or BlackBerry Application Web Loader backs up the encrypted cryptographic services data to a database and stores the database on the user's computer as an .ipd file.

When the update process completes, the BlackBerry Desktop Manager or BlackBerry Application Web Loader restores the cryptographic services data to the BlackBerry device. Only the BlackBerry device that encrypted the cryptographic services data can decrypt the cryptographic services data. The BlackBerry device can decrypt the cryptographic services data only once. The BlackBerry device deletes the BlackBerry services key from the NV store after the BlackBerry device decrypts the cryptographic services data.

The BlackBerry® Enterprise Solution does not back up or restore cryptographic services data except during the BlackBerry Device Software update process from an update web site. When the user backs up or restores BlackBerry device data by selecting the backup and restore options in the BlackBerry Desktop Manager, the back up and restore processes do not access cryptographic services data.

Process flow: Generating a BlackBerry services key that protects cryptographic services data

The BlackBerry® device uses an ephemeral AES-256 encryption key (called the BlackBerry services key) to encrypt the cryptographic services data. To generate the BlackBerry services key, the BlackBerry device performs the following actions:

1. generates a random password from a random source of 32 bytes
2. generates a random salt from a random source of 8 bytes
3. concatenates the salt, password, and salt again into a byte array (for example, `Salt|Password|Salt`)
4. hashes the byte array using SHA-256
5. stores the resulting hash in a byte array that is called a key

```
(key) =
SHA256(Salt|Password|Salt)
```

6. hashes the key 18 more times and stores the result in a key each time
   For example, for i=0 to 18, the BlackBerry device performs the following actions:

```
(key) = SHA256(key)
 i++
 done
```

   The final hash creates the BlackBerry services key.
7. stores the BlackBerry services key in a location of the NV store that third-party applications and the user cannot access

Process flow: Backing up cryptographic services data using the BlackBerry Desktop Manager

1. A user connects a BlackBerry® device to the BlackBerry® Desktop Manager and selects the option to update the BlackBerry® Device Software.
2. The BlackBerry Desktop Manager determines that cryptographic services data require backup during the update process. It sends the BlackBerry device a command to encrypt the cryptographic services data.
3. The BlackBerry device performs the following actions:
   a. generates a BlackBerry services key and stores the BlackBerry services key in the NV store
   b. encrypts the cryptographic services data using the BlackBerry services key
   c. encrypts the BlackBerry services key using the content protection key if you or the user turns on content protection
4. The BlackBerry Desktop Manager backs up the encrypted cryptographic services data in a database on the user's computer as an .ipd file.

Process flow: Restoring cryptographic services data using the BlackBerry Desktop Manager or BlackBerry Application Web Loader

1. After the update process completes, the BlackBerry® Desktop Manager or BlackBerry Application Web Loader determines that cryptographic services data must be restored to the BlackBerry device. The BlackBerry Desktop Manager or BlackBerry Application Web Loader sends a BlackBerry device a command to restore the cryptographic services data.
2. The BlackBerry device performs the following actions:
   a. retrieves the BlackBerry services key and verifies that the BlackBerry services key was not used previously
   b. decrypts the BlackBerry services key if you or a user turn on content protection
3. The BlackBerry Desktop Manager restores the encrypted cryptographic services data to the BlackBerry device.
4. The BlackBerry device performs the following actions:
   a. decrypts the encrypted cryptographic services data using the BlackBerry services key
   b. restores the decrypted cryptographic data
   c. deletes the BlackBerry services key from the NV store

Extending messaging security to a BlackBerry device 14

If your organization's messaging environment supports highly secure messaging technology such as PGP® encryption or S/MIME encryption, you can configure the BlackBerry® Enterprise Solution to encrypt a message using PGP encryption or S/MIME encryption so that the message remains encrypted when the BlackBerry® Enterprise Server forwards the message to the email applications of recipients. To extend messaging security, the sender and recipient must install highly secure messaging technology on the computers that host the email applications and on their BlackBerry devices, and you must configure the BlackBerry devices to use the highly secure messaging technology.

Extending messaging security using PGP encryption

You can extend messaging security for the BlackBerry® Enterprise Solution and permit a BlackBerry device user to send and receive PGP® protected email messages and PGP protected PIN messages on a BlackBerry device. The BlackBerry Enterprise Solution supports the OpenPGP format and PGP/MIME format on the BlackBerry device.

To extend messaging security, you must instruct the BlackBerry device user to install the PGP® Support Package for BlackBerry® smartphones on the BlackBerry device and to transfer the PGP private key of the BlackBerry device user to the BlackBerry device. The BlackBerry device user can use the PGP private key to digitally sign, encrypt, and send PGP protected messages from the BlackBerry device. If a BlackBerry device user does not install the PGP Support Package for BlackBerry smartphones, the BlackBerry device receives PGP protected messages as unreadable ciphertext.

To require the BlackBerry device user to use PGP encryption when forwarding or replying to messages, you can configure the PGP Force Digital Signature IT policy rule and the PGP Force Encrypted Messages IT policy rule.

The PGP Support Package for BlackBerry smartphones is designed to support encoding and decoding Unicode messages and permits PGP encryption using keys or passwords. The PGP Support Package for BlackBerry smartphones permits the BlackBerry device to encrypt PGP protected email messages or PGP protected PIN messages using a password that the sender and recipient both know .

For more information about the OpenPGP format, see RFC 2440. For more information about the PGP/MIME format, see RFC 3156.

For more information about the PGP Support Package for BlackBerry smartphones, see the *PGP Support Package for BlackBerry Devices Security Technical Overview*.

PGP public keys and PGP private keys

The PGP® Support Package for BlackBerry® smartphones uses public key cryptography with PGP public keys and PGP private keys.

Key	Description
PGP public key	The PGP Support Package for BlackBerry smartphones uses the PGP public key of the recipient to encrypt outgoing email messages and the PGP public key of the sender to verify digital signatures on incoming email messages. The PGP public key is designed so that recipients and senders can distribute and access the key without compromising it. The PGP public key is stored typically on the PGP® Universal Server, an LDAP server, or a DSML certificate server.
PGP private key	The PGP Support Package for BlackBerry smartphones uses the PGP private key of the sender to digitally sign outgoing email messages and the PGP private key of the recipient to decrypt incoming email messages. To make sure that security is not compromised, you must make sure that private key information remains private to the key owner. The BlackBerry device stores the PGP private key.

Retrieving PGP keys from a PGP Universal Server, LDAP servers, or DSML certificate servers

If your organization's environment includes a PGP® Universal Server, the administrator of the PGP Universal Server can configure the email policy of the PGP Universal Server. After a user installs the PGP® Support Package for BlackBerry® smartphones, a BlackBerry device can retrieve and enforce the email policy of the PGP Universal Server for all email messages that the user sends.

The BlackBerry device is designed to use the BlackBerry MDS Connection Service to connect to the PGP Universal Server and to any LDAP server or DSML certificate server that a user specifies on the BlackBerry device or that you specify using the BlackBerry Administration Service. The BlackBerry MDS Connection Service uses standard protocols, such as HTTP and TCP/IP, to permit the BlackBerry device to retrieve PGP public keys, PGP key status, and X.509 certificate status from the PGP Universal Server, an LDAP server, or a DSML certificate server over the wireless network. The BlackBerry MDS Connection Service can connect to LDAP servers using LDAPS.

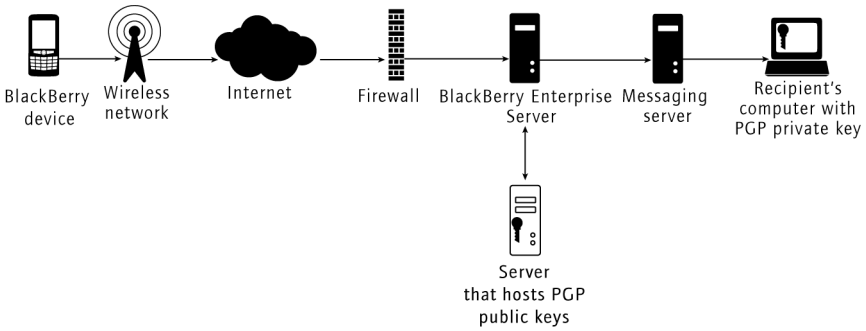
Only BlackBerry® Device Software versions 5.0 and later support DSML certificate servers.

Encryption algorithms that the BlackBerry device supports for PGP encryption

When you turn on PGP® encryption, the default value of the PGP Allowed Content Ciphers IT policy rule specifies that a BlackBerry® device can use any of the following encryption algorithms to encrypt email messages and PIN messages: AES-256, AES-192, AES-128, CAST-128, or Triple DES-168. You can change the value to use a subset of the encryption algorithms if your organization's security policies require it.

The PGP public key of the recipient indicates which encryption algorithm the recipient's email application supports, and the BlackBerry device is designed to use that encryption algorithm. By default, if the PGP public key of the recipient does not include a list of encryption algorithms, the BlackBerry device encrypts the email message or PIN message using Triple DES.

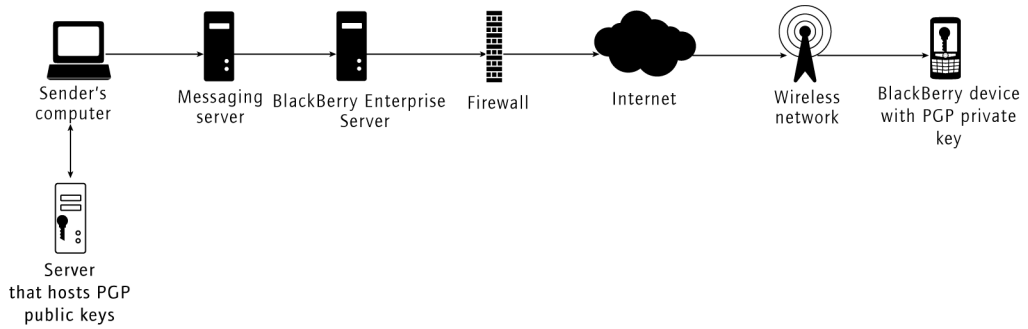
Process flow: Sending an email message using PGP encryption



If a sender installs the PGP® Support Package for BlackBerry® smartphones on a BlackBerry device, the BlackBerry device encrypts outgoing email messages.

1. The BlackBerry device performs the following actions:
   a. uses the BlackBerry MDS Connection Service to retrieve the PGP public key of the recipient from the PGP® Universal Server, LDAP server, or DSML certificate server
   b. encrypts the email message using the PGP public key of the recipient
   c. uses BlackBerry transport layer encryption to encrypt the PGP encrypted message
   d. sends the message that is encrypted using BlackBerry transport layer encryption and PGP encryption to the BlackBerry® Enterprise Server
2. The BlackBerry Enterprise Server removes the BlackBerry transport layer encryption and sends the PGP encrypted message to the recipient.

Process flow: Receiving a PGP encrypted message



If a recipient installs the PGP® Support Package for BlackBerry® smartphones on a BlackBerry device, the BlackBerry device decrypts incoming PGP encrypted messages.

1. A sender uses the PGP technology on the email application to encrypt an email message using the PGP public key of the recipient.
2. The BlackBerry® Enterprise Server performs the following actions:
   a. retrieves the email message from the messaging server
   b. uses BlackBerry transport layer encryption to encrypt the PGP encrypted message
   c. sends the email message encrypted using BlackBerry transport layer encryption and PGP encryption to the BlackBerry device
3. The BlackBerry device performs the following actions:
   a. decrypts the BlackBerry transport layer encryption and stores the PGP encrypted message in the flash memory of the BlackBerry device
   b. decrypts the PGP encrypted message using the PGP private key of the recipient and displays the contents of the email message when the recipient opens the email message on the BlackBerry device

Extending messaging security using S/MIME encryption

You can extend messaging security for the BlackBerry® Enterprise Solution and permit a BlackBerry device user to send and receive S/MIME-protected email messages and S/MIME-protected PIN messages on a BlackBerry device.

To extend messaging security, you must instruct the BlackBerry device user to install the S/MIME Support Package for BlackBerry® smartphones on the BlackBerry device and to transfer the S/MIME private key of the BlackBerry device user to the BlackBerry device. The S/MIME Support Package for BlackBerry smartphones is designed to work with email applications such as Microsoft® Outlook®, Microsoft Outlook Express, and IBM® Lotus Notes®, and with PKIs such as Netscape®, Entrust Authority™ Security Manager version 5 and later, and Microsoft certification authorities.

The BlackBerry device user uses the S/MIME private key to decrypt S/MIME-protected messages on the BlackBerry device and to sign, encrypt, and send S/MIME-protected messages from the BlackBerry device. If the BlackBerry® Enterprise Server receives an S/MIME-protected message but the BlackBerry device user did not install the S/MIME Support Package for BlackBerry smartphones, the BlackBerry Enterprise Server sends a message to the BlackBerry device to indicate that the BlackBerry device does not support S/MIME-protected messages.

After the BlackBerry device user installs the S/MIME Support Package for BlackBerry smartphones, the BlackBerry device user can synchronize and manage S/MIME certificates and S/MIME private keys using the certificate synchronization tool of the BlackBerry® Desktop Manager. The BlackBerry Enterprise Server does not apply an appended disclaimer to S/MIME-protected messages that the BlackBerry device user sends from the BlackBerry device. Digital signatures on S/MIME-protected messages that the BlackBerry device sends are not valid if disclaimers are appended to the messages.

To require the BlackBerry device user to use S/MIME encryption when forwarding or replying to messages, you can configure the S/MIME Force Digital Signature IT policy rule and the S/MIME Force Encrypted Messages IT policy rule.

The S/MIME Support Package for BlackBerry smartphones is also designed to support the following features:

- encoding and decoding of Unicode messages
- ability to use a password, which the sender and recipient each know, to encrypt S/MIME-protected email messages or PIN messages
- ability to read S/MIME certificates that are stored on a smart card

For more information, see the *S/MIME Support Package for BlackBerry Devices Security Technical Overview*.

S/MIME certificates and S/MIME private keys

The S/MIME Support Package for BlackBerry® smartphones uses public key cryptography with S/MIME certificates and S/MIME private keys to encrypt and decrypt email messages and PIN messages. The S/MIME Support Package for BlackBerry smartphones use PKI protocols to search for and retrieve S/MIME certificates and certificate status over the wireless network.

Item	Description
S/MIME certificate	When a user sends an email message or PIN message from a BlackBerry device, the BlackBerry device uses the S/MIME certificate of the recipient to encrypt the message. When a user receives a signed email message or signed PIN message on a BlackBerry device, the BlackBerry device uses the S/MIME certificate of the sender to verify the message signature. S/MIME certificates are stored on LDAP servers or DSML certificate servers.

Item	Description
S/MIME private key	When a user sends a signed email message or signed PIN message from a BlackBerry device, the BlackBerry device hashes the message using SHA-1, SHA-256, SHA-384, SHA-512, or MD5. The BlackBerry device then uses the S/MIME private key of the user to digitally sign the message hash. When a user receives an encrypted email message or encrypted PIN message on a BlackBerry device, the BlackBerry device uses the private key of the user to decrypt the message. The BlackBerry device stores the private key.

Retrieving S/MIME certificates and checking certificate status

The S/MIME Support Package for BlackBerry® smartphones is designed so that the BlackBerry device and the certificate synchronization tool of the BlackBerry® Desktop Manager can perform the following actions:

- use LDAP, LDAPS, or DSML to search for and retrieve S/MIME certificates of recipients from LDAP servers or DSML certificate servers
- use OCSP to check the revocation status of S/MIME certificates
- retrieve the revocation status of S/MIME certificates from a certificate revocation list

S/MIME encryption algorithms

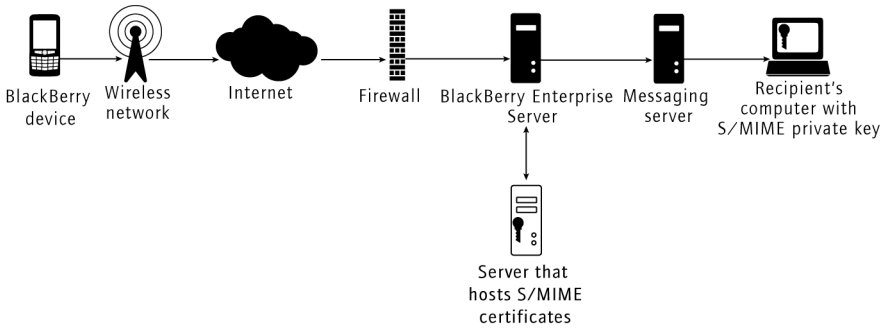
When you turn on S/MIME encryption, the default value of the S/MIME Allowed Content Ciphers IT policy rule specifies that a BlackBerry® device can use any of the following encryption algorithms to encrypt messages: AES-256, AES-192, AES-128, CAST-128, RC2-128, or Triple DES. By default, the BlackBerry device cannot use the RC2-64 algorithm and RC2-40 algorithm to encrypt S/MIME messages. You can change the value of the S/MIME Allowed Content Ciphers IT policy rule to use a subset of the encryption algorithms if your organization's security policies require it.

If a BlackBerry device user wants to send an email message to a recipient that the user previously received an email message from, the BlackBerry device is designed to store the encryption algorithms that the recipient's email application can support, and use one of those encryption algorithms. By default, if the BlackBerry device cannot determine the encryption algorithms that the recipient's email application can support, the BlackBerry device encrypts the email message using Triple DES.

You can use the Weak Digest Algorithms IT policy rule to specify the algorithms that your organization considers to be weak. The BlackBerry device uses the list of weak algorithms in the Weak Digest Algorithms IT policy rule when the BlackBerry device verifies the following information:

- An S/MIME-enabled application did not use a weak algorithm to generate the digital signatures on the email messages that the BlackBerry device receives.
- The certificate chains for the certificates that an S/MIME-enabled application used to digitally sign email messages that the BlackBerry device receives do not contain hash values generated using a weak algorithm.

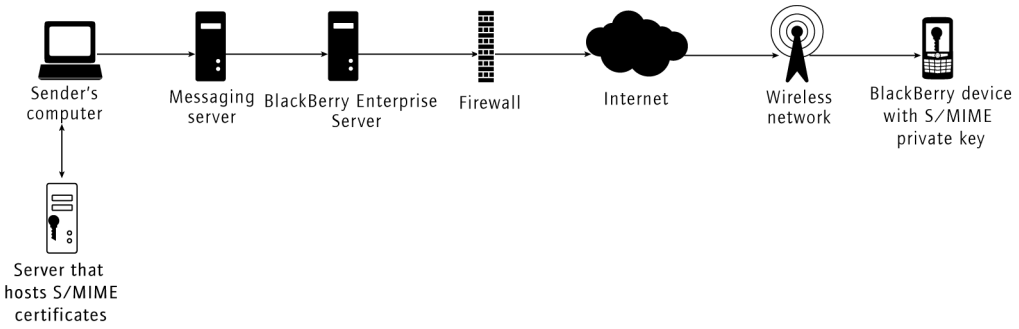
Process flow: Sending an email message using S/MIME encryption



If a sender installs the S/MIME Support Package for BlackBerry® smartphones on a BlackBerry device, the BlackBerry device encrypts outgoing email messages.

1. The BlackBerry device performs the following actions:
   a. uses the BlackBerry MDS Connection Service to retrieve the S/MIME certificate of the recipient from the LDAP server or DSML certificate server and verify the certificate status
   b. encrypts the email message with the S/MIME certificate of the recipient or a password that the sender specifies
   c. if the sender specifies a password, combines the password with random bytes to generate an encryption key that is specific to S/MIME encryption
   d. uses BlackBerry transport layer encryption to encrypt the S/MIME-encrypted message
   e. sends the message that is encrypted using BlackBerry transport layer encryption and S/MIME encryption to the BlackBerry® Enterprise Server
2. The BlackBerry Enterprise Server decrypts the BlackBerry transport layer encryption and sends the S/MIME-encrypted message to the recipient.
3. The recipient decrypts the S/MIME-encrypted message using the S/MIME private key.

Process flow: Receiving an S/MIME-encrypted email message



If a recipient installs the S/MIME Support Package for BlackBerry® smartphones, the BlackBerry device decrypts incoming email messages.

1. The sender uses the S/MIME technology on the email application to encrypt the email message using the S/MIME certificate of the recipient.
2. The BlackBerry® Enterprise Server performs the following actions:
   a. retrieves the S/MIME-encrypted message from the messaging server
   b. encrypts the email message a second time with S/MIME encryption if the email message is signed-only or weakly encrypted and if you turned on the Turn on S/MIME encryption on signed and weakly encrypted messages option in the BlackBerry Administration Service
   c. uses BlackBerry transport layer encryption to encrypt the S/MIME-encrypted message
   d. sends the email message that is encrypted using BlackBerry transport layer encryption and S/MIME encryption to the BlackBerry device
3. The BlackBerry device decrypts the BlackBerry transport layer encryption and stores the S/MIME-encrypted message in BlackBerry device memory.
4. When the recipient opens the email message on the BlackBerry device, the BlackBerry device decrypts the S/MIME-encrypted message using the S/MIME private key of the recipient and displays the message contents. If the email message is encrypted with a password, the recipient types the password to decrypt the S/MIME-encrypted message.

Extending messaging security using IBM Lotus Notes encryption

By default, if your organization's environment includes BlackBerry® Enterprise Server version 4.1 or later for IBM® Lotus® Domino® and IBM® Lotus Notes® API version 7.0 or later, a BlackBerry device can decrypt messages that are encrypted using Lotus Notes encryption.

In BlackBerry Enterprise Server version 5.0 or later and BlackBerry® Device Software version 5.0 or later, a BlackBerry device user can encrypt messages using Lotus Notes encryption. When the BlackBerry device user creates, forwards, or replies to a message, the BlackBerry device user can indicate whether the BlackBerry Enterprise Server must encrypt the message before it sends the message to the recipients.

To use Lotus Notes encryption on the BlackBerry device, the BlackBerry device user must import a copy of the Lotus Notes .id file into the user's message database using the BlackBerry Desktop Software or Lotus® iNotes®. If your organization's environment includes Lotus Domino version 8.5.1 or later and BlackBerry Enterprise Server version 4.1 or later, the BlackBerry Enterprise Server can automatically synchronize the copy of the Lotus Notes .id file on the BlackBerry device with the latest copy that is in the Lotus Notes ID vault. If your organization's environment includes Lotus Domino version 8.5 SP1 or later and BlackBerry Enterprise Server version 5.0 SP1 or later, you can configure the BlackBerry Enterprise Server to import the Lotus Notes .id file automatically into the BlackBerry device from the Lotus Notes ID vault.

To require the BlackBerry device user to use Lotus Notes encryption when forwarding or replying to messages, you can configure the Require Notes Native Encryption For Outgoing Messages IT policy rule. To prevent a BlackBerry device user from forwarding or replying to Lotus Notes protected messages, you can configure the Disable Notes Native Encryption Forward And Reply IT policy rule.

Protecting the password for an IBM Lotus Notes .id file

How a BlackBerry device protects the password for an IBM Lotus Notes .id file

After a user imports an IBM® Lotus Notes® .id file and password for the Lotus Notes .id file to a BlackBerry® device, the BlackBerry device encrypts the password in BlackBerry device memory using AES encryption and the device transport key. The BlackBerry device decrypts the password before it calls the required security functions in the Lotus Notes API.

The BlackBerry device deletes the Lotus Notes .id file and plain-text password from the BlackBerry device memory when it receives a notification from the BlackBerry® Enterprise Server that the BlackBerry Enterprise Server cannot decrypt a message, when the BlackBerry device resets, or when the Lotus Notes password expires. (The default expiration period is 24 hours.) You can use the Native Encryption Password Timeout IT policy rule to specify the maximum duration (in minutes) that the BlackBerry device stores the plain-text password for the Lotus Notes .id file.

You can change the timeout value to 0 to require the user to type the password to decrypt each Lotus Notes encrypted email message that the user receives on the BlackBerry device.

When Lotus Notes encryption is not available, the user can turn on Lotus Notes encryption manually by importing the Lotus Notes .id file or by changing the password using the BlackBerry® Desktop Software or IBM® Lotus® Domino® Web Access client.

How the BlackBerry Messaging Agent protects the password for an IBM Lotus Notes .id file

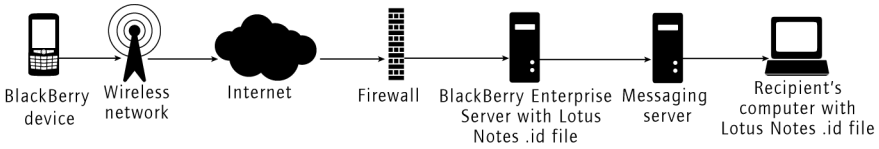
After a user imports an IBM® Lotus Notes® .id file and the password for the Lotus Notes .id file to a BlackBerry® device, the BlackBerry Messaging Agent encrypts the Lotus Notes .id file and password in the BlackBerry Messaging Agent memory cache using AES encryption and the device transport key.

The BlackBerry Messaging Agent deletes the Lotus Notes .id file and the plain-text password when the BlackBerry® Enterprise Server cannot decrypt a message, when the BlackBerry Enterprise Server restarts, or when the password expires. (The default timeout value is 24 hours.)

The BlackBerry Messaging Agent does not delete the encrypted password in the BlackBerry Messaging Agent memory cache. You can change the duration that the BlackBerry Messaging Agent caches the password for. For information about changing the duration that the BlackBerry Messaging Agent caches the password for, visit www.blackberry.com/support to read article KB12420.

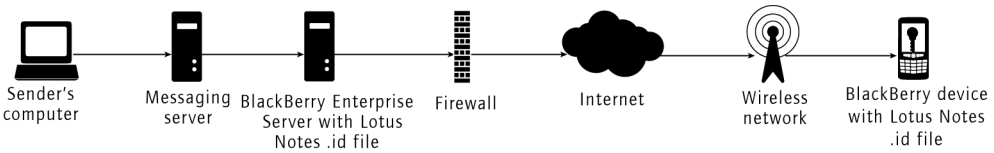
If the user types a password incorrectly more than 10 times consecutively within 1 hour, the BlackBerry Messaging Agent makes secure messaging unavailable for 1 hour. This period increases each time that the user exceeds the maximum number of unsuccessful password attempts. The period increases by 10-minute increments to a maximum of 24 hours. When the user types the password correctly, the BlackBerry Messaging Agent restores the default value of 1 hour.

Process flow: Sending an email message using IBM Lotus Notes encryption



1. A user indicates, using the menu in the messages application, that the BlackBerry® device must encrypt the email message.
2. The BlackBerry device performs the following actions:
   a. prompts the user for the password for the IBM® Lotus Notes® .id file
   b. configures the email message for Lotus Notes encryption
   c. encrypts the email message using BlackBerry transport layer encryption
   d. sends the email message and password to the BlackBerry® Enterprise Server
3. The BlackBerry Enterprise Server decrypts the email message using BlackBerry transport layer encryption.
4. The BlackBerry Messaging Agent on the BlackBerry Enterprise Server decrypts the cached password for the Lotus Notes .id file and validates the password that the BlackBerry device sent. If the BlackBerry Messaging Agent can verify the password, the BlackBerry Messaging Agent uses the password to encrypt the message using Lotus Notes encryption.
5. The BlackBerry Enterprise Server sends the encrypted email message to the messaging server so that the messaging server can deliver it to the recipient.

Process flow: Receiving an IBM Lotus Notes encrypted message



1. A user uses the IBM® Lotus Notes® application on the user's computer to encrypt a message using the password for the Lotus Notes .id file.
2. The BlackBerry® Enterprise Server performs the following actions:
   a. retrieves the Lotus Notes encrypted message from the messaging server
   b. encrypts the Lotus Notes encrypted message using BlackBerry transport layer encryption
   c. sends the encrypted message to the BlackBerry device
3. The BlackBerry device decrypts the message using BlackBerry transport layer encryption and stores the message without decrypting the Lotus Notes encryption.
4. The user tries to open the Lotus Notes encrypted message on the BlackBerry device.
5. The BlackBerry Messaging Agent on the BlackBerry Enterprise Server decrypts the cached password for the Lotus Notes .id file and uses the password to decrypt the message. If the BlackBerry Messaging Agent does not have the password, from the menu in the messages application, the user must select More, More All, or Open Attachment to send the decrypted message to the BlackBerry device.
6. The BlackBerry Enterprise Server deletes the decrypted password from the BlackBerry Messaging Agent memory cache and sends the decrypted message to the BlackBerry device.

Extending messaging security to attachments

The BlackBerry® Enterprise Server supports attachments in PGP® encrypted messages and S/MIME-encrypted messages. It also permits a user to view encrypted attachments on a BlackBerry device. You can use the S/MIME Allowed Encrypted Attachment Mode IT policy rule and the PGP Allowed Encrypted Attachment Mode IT policy rule to specify the least restrictive mode that a BlackBerry device can use to retrieve attachment information that is PGP encrypted or S/MIME encrypted. The BlackBerry device supports OpenPGP format and PGP/MIME format for PGP encryption.

When a user receives an OpenPGP encrypted message that includes an attachment, the BlackBerry Enterprise Server checks the data in the attachment header. The BlackBerry Enterprise Server is designed to send the email message and the encrypted message key to the BlackBerry device automatically.

Process flow: Viewing an attachment in a PGP encrypted message or S/MIME-encrypted message

The S/MIME Allowed Encrypted Attachment Mode IT policy rule or PGP® Allowed Encrypted Attachment Mode IT policy rule determines how a BlackBerry® device responds when it receives a PGP/MIME encrypted message or S/MIME-encrypted message that contains an attachment. These rules determine whether the following actions occur automatically when the user opens the email message, or whether the user must request the actions manually.

1. A BlackBerry device sends the message key and a request for the data in the attachment header to the BlackBerry® Enterprise Server.
2. The BlackBerry Enterprise Server uses the message key to decrypt the email message and access the data in the attachment header. The BlackBerry Enterprise Server sends the data in the attachment header to the BlackBerry device.
3. The BlackBerry device processes the data in the attachment header with the email message and displays the associated attachment information so that the user can select the attachment for viewing.

Process flow: Viewing an attachment that is encrypted using S/MIME encryption, PGP/MIME encryption, or OpenPGP encryption

1. The BlackBerry® device sends the message key and a request for the attachment data to the BlackBerry® Enterprise Server.
2. The BlackBerry Enterprise Server uses the message key to decrypt the email message and access the attachment data that corresponds to the data in the attachment header. The BlackBerry Enterprise Server decrypts the attachment and sends the rendered attachment data to the BlackBerry device.
3. The BlackBerry device displays the attachment.

To protect the decrypted attachment data that the BlackBerry device stores, you can turn on content protection.

Configuring two-factor authentication and protecting Bluetooth connections

15

BlackBerry Smart Card Reader

The BlackBerry® Smart Card Reader is an accessory that, when used in proximity to a Bluetooth® enabled BlackBerry device or a Bluetooth enabled computer, permits a user to authenticate with a smart card and log in to the BlackBerry device or computer.

The BlackBerry Smart Card Reader is designed to perform the following actions:

- communicate with BlackBerry devices and computers using Bluetooth technology version 1.1 or later and, by default, use AES-256 encryption on the application layer
- permit a user to use two-factor authentication to access BlackBerry services and PKI applications
- permit a user to digitally sign and encrypt email messages and receive encrypted messages on the BlackBerry device when the user installs the S/MIME Support Package for BlackBerry® smartphones
- store all encryption keys in RAM only and never write the keys to flash memory

The BlackBerry Smart Card Reader permits a user to use what the user has (smart card) and what the user knows (smart card password) to prove the user's identity to the BlackBerry device or a computer.

For more information, see the *BlackBerry Smart Card Reader Security Technical Overview*.

Advanced Security SD cards

Similar to the BlackBerry® Smart Card Reader, an Advanced Security SD card permits a user to use what the user has (smart card) and what the user knows (smart card password) to prove the user's identity to the BlackBerry device. The BlackBerry® Enterprise Solution supports Advanced Security SD cards that use the security system for the MCEX smart card.

You can configure a BlackBerry device to require that a user uses an Advanced Security SD card to perform the following actions:

- unlock the BlackBerry device and access BlackBerry services and PKI applications using two-factor authentication
- digitally sign and encrypt email messages and PIN messages using S/MIME encryption when the user installs the S/MIME Support Package for BlackBerry® smartphones on the BlackBerry device
- decrypt S/MIME-encrypted email messages and PIN messages
- import certificates that are stored on the Advanced Security SD card into the NV store of the BlackBerry device flash memory
- open SSL connections

To configure the BlackBerry device to support an Advanced Security SD card, a user must insert the Advanced Security SD card into the BlackBerry device and install the smart card driver of the Advanced Security SD card on the BlackBerry device using the BlackBerry® Desktop Manager. After the user installs the smart card driver on the BlackBerry device, the user can configure the driver settings in the security options, on the Smart Card screen.

To control how a BlackBerry device can use an Advanced Security SD card, you can use the Force Smart Card Two-Factor Authentication IT policy rule, Force Smart Card Two Factor Challenge Response IT policy rule, or Disable Certificate or Key Import From External Memory IT policy rule.

To permit third-party applications on the BlackBerry device to access the Advanced Security SD card, a developer can use the SmartCard API in the BlackBerry® Java® Development Environment.

BlackBerry® Device Software versions 5.0 and later support Advanced Security SD cards.

For more information about configuring the BlackBerry device to support an Advanced Security SD card, see the user guide for the BlackBerry device. For more information about using IT policy rules, see the *BlackBerry Enterprise Server Policy Reference Guide*.

Related topics

Managing BlackBerry Java Applications on a BlackBerry device using code signing, 118

Two-factor authentication

You can use the BlackBerry® Smart Card Reader or an Advanced Security SD card to require a user to use a smart card and the smart card password to prove the user's identity before the BlackBerry device unlocks. If a user installs a smart card authenticator, smart card driver, and smart card reader driver on the BlackBerry device, you or the user can configure two-factor authentication on the BlackBerry device to bind the BlackBerry device to the installed smart card. After the BlackBerry device binds to the smart card, the BlackBerry device requires the user to use the smart card to authenticate before the BlackBerry device unlocks.

To require that a user authenticate with the BlackBerry device using the smart card, you can configure the Force Smart Card Two-Factor Authentication IT policy rule in the BlackBerry Administration Service. If you do not require the user to authenticate with the BlackBerry device using a smart card, the user can turn on or turn off two-factor authentication in the BlackBerry device options, in the security options, in the User Authenticator field.

Verifying that a BlackBerry device is bound to a smart card

After a user turns on two-factor authentication, the BlackBerry® device prompts the user to insert the smart card into the BlackBerry® Smart Card Reader. The BlackBerry device displays the label and card type of the bound smart card.

If the BlackBerry device is running BlackBerry® Device Software version 3.6, the smart card information that the BlackBerry device displays when it prompts the user to insert the smart card into the BlackBerry Smart Card Reader is the only indication that a smart card is bound to the BlackBerry device.

If the BlackBerry device is running BlackBerry Device Software version 4.0 or later, the BlackBerry device displays the smart card information when it prompts the user to insert the smart card. The user can view the smart card information in the BlackBerry device options, in the security options. The Initialized field specifies whether the BlackBerry device authenticated with and is bound to the smart card.

Process flow: Turning on two-factor authentication using a smart card

When you or a user turns on two-factor authentication with the BlackBerry® Smart Card Reader, the BlackBerry device performs the following actions:

1. locks
2. prompts the user to type the BlackBerry device password when the user tries to unlock the BlackBerry device
3. requires the user to specify a BlackBerry device password, if the user has not yet specified one
4. prompts the user to type the smart card password to turn on two-factor authentication using the smart card
5. binds to the smart card by storing the following binding information in the NV store in the BlackBerry device memory that the user cannot access:
   - name of a Java® class that the BlackBerry Smart Card Reader requires
   - binding information format for the smart card type (for example, the type for CAC is GSA CAC)
   - name of a Java class that the smart card code requires
   - unique 64-bit identifier that the smart card provides
   - smart card label that the smart card provides (for example, HISLOP.GREG.1234567890)
6. pushes the current IT policy to the BlackBerry Smart Card Reader

Creating two-factor authentication methods

The BlackBerry® Java® Development Environment version 5.0 includes the User Authenticator API that a developer can use to create two-factor authentication methods. A user can use the two-factor authentication methods with the BlackBerry device password to unlock a BlackBerry device. After the developer creates an authentication method using the User Authenticator API, you can install the authentication method on the BlackBerry device using a software configuration.

To configure the BlackBerry device so that the user must provide the BlackBerry device password and authenticate using a two-factor authentication method before the BlackBerry device unlocks, you change the Allowed Authentication Mechanisms IT policy rule to Other and configure the Is Access to the User Authenticator API Allowed application control policy rule.

The User Authenticator API permits a developer to add a field to the password dialog box on the BlackBerry device for the authentication method. You can create as many two-factor authentication methods as the security policies of your organization require.

BlackBerry® Device Software versions 5.0 and later support the User Authenticator API.

For more information about the User Authenticator API, see the *BlackBerry Java Development Environment Fundamentals Guide*.

Two-factor content protection

Content protection is designed to encrypt data on a BlackBerry® device when the BlackBerry device is locked. When you configure two-factor content protection, the BlackBerry device performs the following actions:

- encrypts the user data on the BlackBerry device using the content encryption key
- generates a key using the BlackBerry device password that encrypts the content encryption key
- encrypts the key that the BlackBerry device generates using the private key that is stored on the smart card

You can use either a smart card with the BlackBerry® Smart Card Reader or a microSD smart card to store the private key. The content encryption key is not transferred from the BlackBerry device to the BlackBerry Smart Card Reader or to the microSD smart card.

Two-factor content protection requires the BlackBerry device password, a smart card, and an authentication certificate that is stored on the BlackBerry device. The authentication certificate must contain the public key for the private key that is stored on the smart card. If the authentication certificate expires or is revoked before a user can replace it, the user must delete all BlackBerry device data from the BlackBerry device before the BlackBerry device can recover. This feature is designed to protect the user data on the BlackBerry device if the BlackBerry device is lost or stolen.

You or a user can configure two-factor content protection. By default, if a user has a smart card and an authentication certificate on the BlackBerry device, the user can turn on two-factor content protection. To make two-factor content protection mandatory or optional, or to prevent a user from configuring it, you can use the Two-factor Content Protection Usage IT policy rule. After you or a user turns on two-factor content protection, to unlock the BlackBerry device, the user must type the BlackBerry device password and smart card PIN on the login screen in the appropriate fields.

If you or a user turns on two-factor content protection, you cannot change the BlackBerry device password using the BlackBerry Administration Service. Only the user can change the BlackBerry device password on the BlackBerry device.

BlackBerry® Device Software versions 5.0 and later and BlackBerry Smart Card Reader versions 2.0 and later support two-factor content protection. You must verify that the IT policies that you can use to manage two-factor content protection are available on your organization's BlackBerry® Enterprise Server. BlackBerry Enterprise Server versions 5.0 SP1 and later include the IT policies that you require to manage two-factor content protection.

Unbinding a smart card from a BlackBerry device

When you or a user turns off two-factor authentication, the BlackBerry® device turns off two-factor authentication with the installed smart card. The BlackBerry device also permanently deletes the binding information for the smart card from the BlackBerry device.

When you or the user deletes all BlackBerry device data, the BlackBerry device permanently deletes the smart card binding information from the NV store in flash memory so that a user can authenticate with the BlackBerry device using a new smart card. You can permanently delete the binding information for the smart card from the BlackBerry device by sending the Delete all device data and disable device IT administration command to the BlackBerry device.

Protecting Bluetooth connections on a BlackBerry device

Bluetooth® wireless technology permits a Bluetooth enabled BlackBerry® device to open a wireless connection with other Bluetooth devices that are within a 10-meter range (for example, a hands-free car kit or wireless headset).

The BlackBerry device creates a Bluetooth profile, which specifies how applications on the BlackBerry device and on other Bluetooth devices connect and communicate. The BlackBerry device uses the Bluetooth profile to open serial connections to Bluetooth enabled devices using virtual serial ports.

You can use IT policies to manage a Bluetooth enabled BlackBerry device. By default, a Bluetooth enabled BlackBerry device that runs BlackBerry® Desktop Software version 4.0 or later includes the following security measures:

- You or a user can turn off the Bluetooth wireless technology for the BlackBerry device.
- The user must request a connection or pairing on the BlackBerry device with another Bluetooth device and type a passkey (also known as a shared secret key) to complete the pairing.
- The user can specify whether to encrypt data sent to and from the BlackBerry device over a Bluetooth connection. The BlackBerry® Enterprise Solution uses the passkey to generate encryption keys.
- The BlackBerry device prompts the user each time a Bluetooth device tries to connect to the BlackBerry device.

For more information, see *Security for BlackBerry Devices with Bluetooth Wireless Technology*.

Using CHAP to open a Bluetooth connection between the BlackBerry Desktop Software and a BlackBerry device

A Bluetooth® enabled BlackBerry® device can use CHAP to open a Bluetooth connection to the BlackBerry® Desktop Software. To open a Bluetooth connection, the BlackBerry device or BlackBerry Desktop Software can use CHAP to send a challenge. The BlackBerry device or BlackBerry Desktop Software can subsequently use the SHA-1 algorithm to calculate a response to the challenge or to validate the response of the other party, depending on which party started the process to open the Bluetooth connection.

When the BlackBerry device uses CHAP, the BlackBerry device never sends the BlackBerry device password over an unprotected connection. The BlackBerry device combines the challenge with the BlackBerry device password to authenticate with the BlackBerry Desktop Software.

For more information about CHAP, see RFC 1994.

Wi-Fi enabled BlackBerry devices

16

Wi-Fi® enabled BlackBerry® devices permit users with qualifying data plans to access BlackBerry services over a mobile network, Wi-Fi network, or both networks simultaneously.

When users can access a mobile network and Wi-Fi network simulaneously, users can perform multiple tasks over both networks. For example, a user with a BlackBerry® 8820 smartphone can send messages over a Wi-Fi network and can make a call over the mobile network at the same time.

If users' mobile network providers make UMA technology (GAN technology) available, and users have subscribed to the UMA feature, Wi-Fi enabled BlackBerry devices can access the mobile network providers' voice services and data services over a mobile network or a Wi-Fi network.

Wi-Fi enabled BlackBerry devices can open a Wi-Fi connection from an enterprise Wi-Fi network or, with a VPN session, from a home Wi-Fi network or Wi-Fi hotspot to connect directly to the BlackBerry Router.

Wi-Fi enabled BlackBerry devices are designed to open a connection to the BlackBerry® Internet Service to access the BlackBerry MDS Connection Service, BlackBerry® Messenger, and other BlackBerry devices for PIN messaging. You can verify with your organization's wireless service provider whether your organization's service plan provides access to these services over a Wi-Fi network.

Types of Wi-Fi networks

Wi-Fi® enabled BlackBerry® devices can access BlackBerry services using enterprise Wi-Fi networks, home Wi-Fi networks, or hotspots.

Type	Description
enterprise Wi-Fi networks	An enterprise Wi-Fi network has multiple wireless access points to provide ubiquitous coverage, hotspot coverage, or ubiquitous and hotspot coverage. You can use a Wi-Fi enabled BlackBerry device in any coverage area. You can configure an enterprise Wi-Fi network to require layer 2 authentication. An organization might consider an enterprise Wi-Fi network to be untrusted and require that all Wi-Fi connections to the organization's network occur through a VPN concentrator. You must configure Wi-Fi enabled BlackBerry devices to support the authentication type that your organization uses. An enterprise Wi-Fi network permits optimized access to the BlackBerry® Enterprise Server over a direct IP connection to the BlackBerry Router.

Type	Description
home Wi-Fi networks	A home Wi-Fi network uses a single access point to provide Internet access through a broadband gateway. The broadband gateway can implement NAT and permit VPN connections through the firewall. You can configure a home Wi-Fi network with layer 2 security and password authentication. You must configure BlackBerry devices to support the authentication that the home Wi-Fi network requires. A home Wi-Fi network permits users to access all BlackBerry services from Wi-Fi enabled BlackBerry devices using the BlackBerry® Infrastructure.
hotspots	A hotspot offered by an ISP, a mobile network provider, or a property owner can provide a Wi-Fi connection in public and semipublic areas. The network can be an open network without layer 2 security and use a captive portal for authentication. The captive portal blocks all network traffic except traffic that uses HTTP and it redirects HTTP requests to a login page. After a user logs in to the hotspot, the captive portal permits the user to access wireless network services. Hotspots can use a firewall and they can permit VPN connections. A hotspot permits users to access all BlackBerry services from their Wi-Fi enabled BlackBerry devices using the BlackBerry Infrastructure.

Security features of a Wi-Fi enabled BlackBerry device

Feature	Description
activation of BlackBerry® devices over an enterprise Wi-Fi® network	Activation of BlackBerry devices over an enterprise Wi-Fi network is designed to simplify the actions of activating or updating BlackBerry devices.
authenticated connection with BlackBerry Router	An authenticated connection with a BlackBerry Router permits BlackBerry devices to open a direct connection to the BlackBerry® Enterprise Server after they authenticate with the BlackBerry Router. BlackBerry devices connected to an enterprise Wi-Fi network do not use an SRP connection to send data to the BlackBerry Enterprise Server.

Feature	Description
BlackBerry transport layer encryption	BlackBerry transport layer encryption is designed to encrypt messages that the BlackBerry device and the BlackBerry Enterprise Server send between each other after they open an authenticated connection.
direct access to the BlackBerry® Infrastructure over a Wi-Fi connection	Direct access to the BlackBerry Infrastructure over a Wi-Fi connection permits Wi-Fi enabled BlackBerry devices to access BlackBerry services over the Internet, even if UMA is not available. You can verify with your organization's wireless service provider that your organization's service plan supports access to BlackBerry services over a Wi-Fi connection.
encrypted communication over the Wi-Fi network	BlackBerry devices support multiple security methods that are designed to encrypt communication over the enterprise Wi-Fi network between the BlackBerry device and wireless access points or a network firewall on the enterprise Wi-Fi network.
expanded groups of Wi-Fi and VPN configuration settings	Expanded groups of Wi-Fi and VPN configuration settings permit you to control Wi-Fi connections from BlackBerry devices.
limited connections	Wi-Fi enabled BlackBerry devices are designed to reject incoming connections, to support limited connections in infrastructure mode only, and to prevent ad-hoc mode (also known as peer-to-peer) connections.
multiple Wi-Fi and VPN profiles	Multiple Wi-Fi and VPN profiles are designed to address user requirements in a variety of different environments.
proxy server	The BlackBerry device supports the use of a transparent proxy server that you can configure between the enterprise Wi-Fi network and the BlackBerry device.
software token provisioning	Software token provisioning is designed to permit you to provision and manage the seed for software token authentication (for example, for VPN connections) centrally on BlackBerry devices. The BlackBerry Enterprise Server is designed to work with the RSA® Authentication Manager to provide software token support for use with layer 2 and layer 3 authentication on supported BlackBerry devices.
user-specific configuration settings and IT policy rules	User-specific configuration settings and IT policy rules are designed to simplify the configuration of user-specific Wi-Fi and VPN information (such as user IDs and passwords).
wireless backup of Wi-Fi and VPN profiles	Wireless backup of Wi-Fi and VPN profiles on BlackBerry devices over a Wi-Fi connection permits users to restore the profiles, if necessary.

Feature	Description
wireless software updates	Wireless software updates permits users to update the BlackBerry® Device Software without using the BlackBerry® Desktop Manager or first downloading the software update to a computer.

Protecting a connection between a Wi-Fi enabled BlackBerry device and an enterprise Wi-Fi network

A Wi-Fi® enabled BlackBerry® device is designed to connect to enterprise Wi-Fi networks that use the IEEE® 802.11® standard. The IEEE® 802.11i™ standard uses the IEEE® 802.1X™ standard for authentication and key management to protect enterprise Wi-Fi networks. The IEEE 802.11i standard specifies that organizations must use the PSK protocol or the IEEE 802.1X standard as the access control methods for Wi-Fi networks.

When you configure a Wi-Fi enabled BlackBerry device to use an enterprise Wi-Fi network, you must configure the enterprise Wi-Fi network and BlackBerry device to protect all message data and application data that the BlackBerry® Enterprise Server and BlackBerry device send to each other. For example, to help protect data, you can configure the BlackBerry device to authenticate with the enterprise Wi-Fi network before the BlackBerry device can access the enterprise Wi-Fi network. You can also configure the BlackBerry device and the enterprise Wi-Fi network to encrypt any communication that they send to each other.

For more information about protecting an enterprise Wi-Fi network, see the documentation from your organization's Wi-Fi solution provider.

How a Wi-Fi enabled BlackBerry device can connect to the BlackBerry Infrastructure

A Wi-Fi® enabled BlackBerry® device can connect directly to the BlackBerry® Infrastructure over the Internet to access the data services that a wireless service provider offers, even if UMA is not available. If UMA is available, the BlackBerry device can also access the voice services. A direct connection from the BlackBerry device to the BlackBerry Infrastructure is an alternative to the connection from the BlackBerry device to the BlackBerry Infrastructure over the mobile network. If a user's wireless service provider makes UMA technology (also known as GAN technology) available, and the user subscribes to the UMA feature, the BlackBerry device is designed to open an SSL connection to the GANC using an IPSec VPN tunnel over an enterprise Wi-Fi network.

The BlackBerry device and BlackBerry Infrastructure send all data to each other over an SSL connection. The SSL connection is designed to encrypt the data that the BlackBerry device and BlackBerry Infrastructure send between each other.

How an SSL connection between a Wi-Fi enabled BlackBerry device and the BlackBerry Infrastructure protects data

An SSL connection between a Wi-Fi® enabled BlackBerry® device and the BlackBerry® Infrastructure is designed to provide the same protection that an SRP connection between the BlackBerry® Enterprise Server and BlackBerry Infrastructure provides. It is designed so that a potentially malicious user cannot use the SSL connection to send data to or receive data from the BlackBerry device.

If a potentially malicious user tries to impersonate the BlackBerry Infrastructure, the BlackBerry device is designed to prevent the connection. The BlackBerry device verifies whether the public key of the SSL certificate of the BlackBerry Infrastructure matches the private key of the root certificate that is preloaded on the BlackBerry device during the manufacturing process. If a user accepts a certificate that is not valid, the connection cannot open unless the BlackBerry device can also authenticate with a valid BlackBerry Enterprise Server or valid BlackBerry® Internet Service.

Process flow: Opening an SSL connection between the BlackBerry Infrastructure and a Wi-Fi enabled BlackBerry device

1. A Wi-Fi® enabled BlackBerry® device sends a request to the BlackBerry® Infrastructure to open an SSL connection.
2. The BlackBerry Infrastructure sends its SSL certificate to the BlackBerry device.
3. The BlackBerry device uses a root certificate that is preloaded on the BlackBerry device to verify the SSL certificate. If the user deleted the root certificate, the BlackBerry device prompts the user to trust the SSL certificate.
4. The BlackBerry device opens the SSL connection.

Cipher suites that a Wi-Fi enabled BlackBerry device supports for opening SSL connections and TLS connections

A Wi-Fi® enabled BlackBerry® device supports various cipher suites for direct mode SSL/TLS when the BlackBerry device opens SSL connections or TLS connections to the BlackBerry® Infrastructure or to web servers that are external to your organization.

The BlackBerry device supports the following cipher suites, in order, when it opens SSL connections:

- SSL_RSA_WITH_RC4_128_SHA
- SSL_RSA_WITH_RC4_128_MD5
- SSL_DHE_RSA_WITH_3DES_EDE_CBC_SHA
- SSL_DHE_DSS_WITH_3DES_EDE_CBC_SHA
- SSL_RSA_WITH_3DES_EDE_CBC_SHA
- SSL_DHE_RSA_WITH_DES_CBC_SHA
- SSL_DH_anon_WITH_RC4_128_MD5
- SSL_DHE_DSS_WITH_DES_CBC_SHA
- SSL_RSA_WITH_DES_CBC_SHA

- SSL_DH_anon_WITH_3DES_EDE_CBC_SHA
- SSL_RSA_EXPORT_WITH_RC4_40_MD5
- SSL_DH_RSA_EXPORT_WITH_DES40_CBC_SHA
- SSL_DHE_DSS_EXPORT_WITH_DES40_CBC_SHA
- SSL_RSA_EXPORT_WITH_DES40_CBC_SHA
- SSL_DH_anon_WITH_DES_CBC_SHA
- SSL_DH_anon_EXPORT_WITH_RC4_40_MD5
- SSL_DH_anon_EXPORT_WITH_DES40_CBC_SHA

The BlackBerry device supports the following cipher suites, in order, when it opens TLS connections:

- TLS_DHE_RSA_WITH_AES_128_CBC_SHA
- TLS_DHE_DSS_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA
- TLS_DHE_DSS_WITH_AES_256_CBC_SHA
- TLS_RSA_WITH_AES_256_CBC_SHA
- TLS_RSA_WITH_RC4_128_SHA
- TLS_RSA_WITH_RC4_128_MD5
- TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
- TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA
- TLS_RSA_WITH_3DES_EDE_CBC_SHA
- TLS_DH_anon_WITH_AES_128_CBC_SHA
- TLS_DH_anon_WITH_AES_256_CBC_SHA
- TLS_DH_anon_WITH_RC4_128_MD5
- TLS_DH_anon_WITH_3DES_EDE_CBC_SHA
- TLS_DHE_RSA_WITH_DES_CBC_SHA
- TLS_DHE_DSS_WITH_DES_CBC_SHA
- TLS_RSA_WITH_DES_CBC_SHA
- TLS_RSA_EXPORT_WITH_RC4_40_MD5
- TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA
- TLS_DHE_DSS_EXPORT_WITH_DES40_CBC_SHA
- TLS_RSA_EXPORT_WITH_DES40_CBC_SHA
- TLS_DH_anon_WITH_DES_CBC_SHA
- TLS_DH_anon_EXPORT_WITH_RC4_40_MD5
- TLS_DH_anon_EXPORT_WITH_DES40_CBC_SHA

Managing how a BlackBerry device connects to an enterprise Wi-Fi network

To manage how a Wi-Fi® enabled BlackBerry® device connects to an enterprise Wi-Fi network, you can use IT administration commands, IT policy rules, and configuration settings. You can turn on or turn off Wi-Fi access for the BlackBerry device in BlackBerry® Enterprise Server version 4.1 SP3 or later, and manage Wi-Fi configuration settings and VPN configuration settings for user accounts in BlackBerry Enterprise Server version 4.1 SP2 or later.

When you configure an IT policy or configuration setting, a user cannot override the value on the BlackBerry device.

At an application level, you can specify the types of connections that an application can make. When you configure application control policies, you can control whether the application can access the enterprise Wi-Fi network.

For more information about specifying whether an application can access an enterprise Wi-Fi network, see *Protecting the BlackBerry Device Platform Against Malware*. For more information about using IT policy rules and configuration settings, see the *BlackBerry Enterprise Server Administration Guide* and the *BlackBerry Enterprise Server Policy Reference Guide* .

How the BlackBerry Enterprise Solution protects sensitive Wi-Fi information

To permit a Wi-Fi® enabled BlackBerry® device to access a Wi-Fi network, you must send sensitive Wi-Fi information such as encryption keys and passwords to the BlackBerry device using Wi-Fi profiles, VPN profiles, and IT policy rules. After the BlackBerry device receives the sensitive Wi-Fi information, the BlackBerry device encrypts the encryption keys and passwords and stores them in flash memory in an area that third-party applications cannot access.

The BlackBerry® Enterprise Server encrypts the sensitive Wi-Fi information that it sends to the BlackBerry device and stores the sensitive Wi-Fi information in the BlackBerry Configuration Database. You can help protect the sensitive Wi-Fi information in the BlackBerry Configuration Database using access controls and configuration settings.

Using a VPN with a Wi-Fi enabled BlackBerry device

If your organization's environment includes VPNs, such as IPSec VPNs, you can configure a Wi-Fi® enabled BlackBerry® device to authenticate with the VPN so that it can access an enterprise Wi-Fi network. A VPN provides an encrypted tunnel between a BlackBerry device and your organization's network. VPN is the only layer 3 security method that the BlackBerry device supports.

A VPN solution consists of a VPN client on the BlackBerry device and a VPN concentrator. The BlackBerry device can use the VPN client to authenticate with a VPN concentrator, which acts as the gateway to the enterprise Wi-Fi network. Each BlackBerry device includes a built-in VPN client that supports several VPN concentrators. The VPN client on the BlackBerry device is designed to use strong encryption to authenticate itself with the VPN concentrator. It creates an encrypted tunnel between the BlackBerry device and VPN concentrator that the BlackBerry device and enterprise Wi-Fi network can use to communicate.

After you configure a VPN, the BlackBerry device can use a layer 2 security method to connect to the enterprise Wi-Fi network, and use the VPN to provide authentication with the enterprise Wi-Fi network. In this scenario, you can configure the enterprise Wi-Fi network as an untrusted network, and specify that only a VPN concentrator can connect to the enterprise Wi-Fi network.

Unlike other supported security methods for enterprise Wi-Fi networks, a VPN does not use the wireless access point during data encryption.

For a list of supported VPN concentrators, visit www.blackberry.com/support to read article KB13354.

Permitting a Wi-Fi enabled BlackBerry device to log in to a VPN concentrator

To permit a Wi-Fi® enabled BlackBerry® device to log in to a VPN concentrator automatically after it connects to an enterprise Wi-Fi network, you or a user can configure a VPN profile that includes a user name and password for authentication with the VPN concentrator. Depending on your organization's security policy, you or the user can save the user name and password for authentication with the VPN concentrator on the BlackBerry device. When you or the user saves the user name and password, the BlackBerry device does not prompt the user for the user name and password the first time or each time that the BlackBerry device connects to the enterprise Wi-Fi network.

The BlackBerry device is also compatible with VPN environments that use two-factor authentication using hardware tokens or software tokens for credentials. When the BlackBerry device tries to log in to the VPN, the BlackBerry device uses credentials that the token generates or that the user provides.

For more information about configuring VPN profiles, see the *BlackBerry Enterprise Server Administration Guide*.

Using a segmented network to reduce the spread of malware on an enterprise Wi-Fi network that uses a VPN

When a Wi-Fi® enabled BlackBerry® device connects to an enterprise Wi-Fi network that uses a VPN, the BlackBerry device might permit the VPN concentrator to send data directly to a BlackBerry® Enterprise Server over your organization's network. The VPN concentrator sends data over port 4101. In this scenario, only the VPN concentrator connects to the enterprise Wi-Fi network.

To configure your organization's VPN concentrator to prevent it from opening unnecessary connections to your organization's network, you can configure a segmented network. In a segmented network, you can divide components of your organization's network using firewalls to reduce the spread of malware.

For more information about reducing the spread of malware, see *Protecting the BlackBerry device platform against malware*.

Using a captive portal to connect to an enterprise Wi-Fi network or Wi-Fi hotspot

A captive portal uses web-based authentication to permit a Wi-Fi® enabled BlackBerry® device to connect to an enterprise Wi-Fi network or Wi-Fi hotspot. The BlackBerry device can use a captive portal to access an IP segment of the enterprise Wi-Fi network or Wi-Fi hotspot. After the BlackBerry device connects to the enterprise Wi-Fi network or Wi-Fi hotspot, the user can browse to an HTML login page for a web site that permits the enterprise Wi-Fi network or Wi-Fi hotspot to authenticate with the BlackBerry device before the BlackBerry device can access the web site.

If your organization uses a captive portal, you can permit a user to access the captive portal using the WLAN Login browser on the BlackBerry device. The user must authenticate with the WLAN Login browser using the login information that you provide.

When the BlackBerry device authenticates with the captive portal, the user can use the BlackBerry® Browser on the BlackBerry device to access other web sites and data services that are available on the enterprise Wi-Fi network or Wi-Fi hotspot.

Protecting a connection between a Wi-Fi enabled BlackBerry device and an enterprise Wi-Fi network using RSA authentication

You can use software tokens to provide layer 2 authentication or layer 3 authentication on a Wi-Fi® enabled BlackBerry® device. When you configure a software token for a user, the BlackBerry device is designed to use the passcode to authenticate the user to the Wi-Fi network using PEAP authentication, EAP-GTC authentication, EAP-FAST authentication, EAP-TTLS authentication, or a VPN.

The RSA SecurID® Library on the BlackBerry device permits the BlackBerry device to periodically generate token codes for a software token. The BlackBerry device imports a seed, which consists of random data, and uses the seed to initialize the software token algorithm. The software token algorithm generates the token code on the BlackBerry device.

When the user opens a Wi-Fi connection or VPN connection that requires two-factor authentication on the BlackBerry device, the BlackBerry device prompts the user to type the software token PIN. The RSA SecurID Library adds the software token PIN to the beginning of the token code to create a passcode that the BlackBerry device can use with a two-factor authentication process.

BlackBerry transport layer encryption is designed to protect the seed when the BlackBerry® Enterprise Server sends it over the transport layer. The BlackBerry device uses Research In Motion® proprietary protocols that are designed to be highly secure to perform all communication necessary to retrieve the seed on behalf of the RSA SecurID Library.

Process flow: Generating a token code for a software token

1. An administrator of the RSA SecurID® uses the RSA® Authentication Manager to import a seed as a soft token file in .asc format to a software token database and issue the software token file in .sdtid format. If necessary, the administrator can perform one or more of the following actions:

- permit the user to specify the software token PIN
- configure the RSA SecurID to automatically generate and send a software token PIN to a Wi-Fi® enabled BlackBerry® device
- require the user to specify the software token PIN the first time that the user tries to complete RSA authentication on the BlackBerry device
- bind the seed to a specific BlackBerry device PIN
- specify a password to encrypt the .sdtid file seed

2. You assign the .sdtid file seed for the BlackBerry device to the user account in the BlackBerry Administration Service. If required, you can type the password to decrypt the seed to use it on the BlackBerry device.
3. The BlackBerry® Enterprise Server performs the following actions:
   a. The BlackBerry Enterprise Server stores the .sdtid file seed in the BlackBerry Configuration Database.
   b. The BlackBerry Enterprise Server pushes the .sdtid file seed (and the password, if the administrator of the RSA SecurID specified one) to the BlackBerry device during the BlackBerry device activation process and each time the administrator of the RSA SecurID changes the .sdtid file seed for the BlackBerry device.
4. The BlackBerry device performs the following actions:
   a. The BlackBerry device imports the .sdtid file seed. If the administrator of the RSA SecurID specified a password in the RSA Authentication Manager to encrypt the .sdtid file seed, the BlackBerry device uses the password to decrypt the .sdtid file seed. If the administrator of the RSA SecurID specified that the .sdtid file seed must bind to a specific BlackBerry device PIN, only the BlackBerry device with the specific PIN can import the seed.
   b. The BlackBerry device stores the .sdtid file seed in flash memory.
   c. The BlackBerry device imports a copy of the .sdtid file seed into the RSA SecurID on the BlackBerry device. When the BlackBerry device imports the .sdtid file seed into the RSA SecurID, the RSA SecurID randomly generates a password to encrypt the .sdtid file seed.
5. The RSA SecurID library on the BlackBerry device authenticates with the RSA® Authentication Agent and initializes the software token algorithm one time each minute.
6. Each time the user tries to open a Wi-Fi connection or VPN connection that requires RSA authentication, the BlackBerry device uses the initialized algorithm to combine the .sdtid file seed with random data that is based on the BlackBerry device time and generate a new token code for the software token.
   The administrator of the RSA SecurID can use RSA Authentication Manager version 6.1 or later to configure an optional password to issue an encrypted .sdtid file seed to the user. The RSA SecurID library on the BlackBerry device can decrypt the .sdtid file seed using an optional password. The RSA SecurID library uses code signing to help prevent third-party applications from changing or reading the information that the RSA SecurID library stores on the BlackBerry device.

17 Layer 2 security methods that a Wi-Fi enabled BlackBerry device supports

You can configure a Wi-Fi® enabled BlackBerry® device to use security methods for layer 2 (also known as the IEEE® 802.11™ link layer) so that the BlackBerry device and a wireless access point can encrypt data that they send between them and authenticate the user. The BlackBerry device supports the following layer 2 security methods:

- open (no security method) WEP encryption (64-bit and 128-bit)
- PSK protocol
- IEEE® 802.1X™ standard and EAP authentication using EAP-FAST, EAP-SIM, EAP-TLS EAP-TTLS, LEAP, and PEAP
- TKIP and AES-CCMP encryption for WPA™-Personal, WPA2™-Personal, WPA™-Enterprise, and WPA2™-Enterprise

To support layer 2 security methods, the BlackBerry device has a built-in IEEE 802.1X supplicant.

If your organization's enterprise Wi-Fi network uses EAP authentication, you can permit and deny BlackBerry device access to the enterprise Wi-Fi network by updating your organization's central authentication server. You are not required to update the configuration of each access point.

For more information about IEEE 802.11 and IEEE 802.1X, see www.ieee.org/portal/site. For more information about EAP authentication, see RFC 3748.

WEP encryption

WEP encryption requires a matching encryption key at a wireless access point and on a Wi-Fi® enabled BlackBerry® device to protect the connection to the enterprise Wi-Fi network. The encryption key can be 40 bits in length (for 64-bit WEP encryption) or 104 bits in length (for 128-bit WEP encryption).

By current industry standards, WEP encryption is not a cryptographically strong security solution. WEP encryption weaknesses include the following scenarios:

- A potentially malicious user might capture transmissions over the wireless network and might deduce WEP encryption keys in very little time.
- A potentially malicious user might use a man-in-the-middle attack to change packets that are encrypted using WEP encryption.

You can use a VPN to provide data confidentially if your organization uses WEP encryption. A VPN can authenticate and encrypt access to your organization's network. To configure a BlackBerry device to use WEP encryption, you must send WEP encryption keys to the BlackBerry device using IT policy rules or configuration settings.

For more information about configuring WEP encryption, see the *BlackBerry Enterprise Server Administration Guide*.

PSK protocol

The IEEE® 802.1X™ standard specifies the PSK protocol as an access control method for enterprise Wi-Fi® networks. You can also use the PSK protocol in small-office environments and home environments where it is not feasible to configure server-based authentication.

To configure the PSK protocol, you must send a passphrase that matches the key or passphrase for the wireless access points to a Wi-Fi enabled BlackBerry® device. The access points and BlackBerry device use a passphrase to generate layer 2 encryption keys. The passphrase can be up to 256 bits. All access points and each BlackBerry device in your organization must share the same passphrase.

The PSK protocol is designed to use TKIP keys or AES-CCMP keys to protect communications over the enterprise Wi-Fi network. The PSK protocol relies on the passphrase to control whether a Wi-Fi enabled device (such as a computer or BlackBerry device) can access the enterprise Wi-Fi network.

The BlackBerry device is compatible with the WPA™-Personal and WPA2™-Personal specifications.

For more information about configuring the BlackBerry device to support the PSK protocol, see the *BlackBerry Enterprise Server Administration Guide*.

IEEE 802.1X standard

The IEEE® 802.1X™ standard defines a generic authentication framework that a Wi-Fi® enabled BlackBerry® device and an enterprise Wi-Fi network can use to authenticate with each other.

The IEEE 802.1X standard uses EAP authentication methods to provide mutual authentication between the BlackBerry device and enterprise Wi-Fi network. To act as a Wi-Fi supplicant, the BlackBerry device uses EAP authentication methods that are specified in RFC 3748 and that meet the requirements of RFC 4017. The BlackBerry device uses an EAP authentication method (for example, EAP-TLS, EAP-TTLS, EAP-FAST, or PEAP) and credentials to provide mutual authentication with the enterprise Wi-Fi network, as defined in the WPA™-Enterprise and WPA2™-Enterprise specifications.

Caching a PMK when using the IEEE 802.1X standard

When a Wi-Fi® enabled device (such as a computer or BlackBerry® device) uses the IEEE® 802.11i™ standard with the IEEE® 802.1X™ standard, the key exchange that occurs during EAP authentication generates keying material. A Wi-Fi enabled device and a wireless access point use the keying material when they create the PMK.

A Wi-Fi enabled BlackBerry device and an access point can cache the PMK. The PMK caching process reuses previously generated keying material to skip EAP authentication during subsequent connections and permits the BlackBerry device and an access point to generate session keys. PMK caching helps reduce the roaming latency for the BlackBerry device between access points in an enterprise Wi-Fi network.

Process flow: Authenticating a Wi-Fi enabled BlackBerry device with an enterprise Wi-Fi network using the IEEE 802.1X standard

If you configured a wireless access point to use the IEEE® 802.1X™ standard, the access point permits communication using EAP authentication only. This process flow assumes that you configured a Wi-Fi® enabled BlackBerry® device to use an EAP authentication method to communicate with the access point.

1. The Wi-Fi enabled BlackBerry device associates itself with the access point that you configured to use the IEEE 802.1X standard. The BlackBerry device sends its credentials (typically a user name and password) to the access point.
2. The access point sends the credentials to the authentication server.
3. The authentication server performs the following actions:
   a. authenticates the BlackBerry device on behalf of the access point
   b. instructs the access point to permit access to the enterprise Wi-Fi network
   c. sends Wi-Fi credentials to the BlackBerry device to permit it to authenticate with the access point
4. The access point and BlackBerry device use EAPoL-Key messages to generate encryption keys (for example, WEP, TKIP, or AES-CCMP, depending on the EAP authentication method that the BlackBerry device uses).
   When the BlackBerry device sends EAPoL messages, the BlackBerry device uses the encryption and integrity requirements that the EAP authentication method specifies. When the BlackBerry device sends EAPoL-Key messages, the BlackBerry device uses the ARC4 algorithm or AES algorithm to provide integrity and encryption.

After the access point and BlackBerry device generate the encryption key, the BlackBerry device can access the enterprise Wi-Fi network.

EAP authentication methods that a Wi-Fi enabled BlackBerry device supports

LEAP authentication

LEAP authentication uses the IEEE® 802.1X™ standard and is designed to improve WEP authentication. You can use this authentication method to authenticate a Wi-Fi® enabled BlackBerry® device with an enterprise Wi-Fi network, generate WEP encryption keys that are unique to the BlackBerry device, and configure the enterprise Wi-Fi network to update the WEP encryption keys automatically during a session with the BlackBerry device.

The BlackBerry device supports using LEAP authentication with a user name and password. The BlackBerry device uses a one-way function to encrypt the password before it sends the password to the authentication server on the enterprise Wi-Fi network.

LEAP authentication does not provide mutual authentication between the BlackBerry device and enterprise Wi-Fi network. You can configure password policies on an enterprise Wi-Fi network that require the BlackBerry device to use LEAP authentication to connect to the enterprise Wi-Fi network.

PEAP authentication

PEAP authentication permits a Wi-Fi® enabled BlackBerry® device to authenticate with an authentication server and access an enterprise Wi-Fi network. PEAP authentication uses TLS to create an encrypted tunnel between the BlackBerry device and the authentication server. It uses the TLS tunnel to send the authentication credentials of the BlackBerry device to the authentication server.

The BlackBerry device supports PEAPv0 and PEAPv1 for PEAP authentication. The BlackBerry device also supports EAP-MS-CHAPv2 and EAP-GTC as second-phase protocols during PEAP authentication so that the BlackBerry device can exchange credentials with the enterprise Wi-Fi network.

To configure PEAP authentication, you must install a root certificate on the BlackBerry device that corresponds to the authentication server certificate.

For more information, see the *BlackBerry Enterprise Server Administration Guide*.

EAP-TLS authentication

EAP-TLS authentication uses a PKI to permit a Wi-Fi® enabled BlackBerry® device to authenticate with an authentication server and access an enterprise Wi-Fi network. EAP-TLS authentication uses TLS to create an encrypted tunnel between the BlackBerry device and the authentication server. EAP-TLS authentication uses the TLS encrypted tunnel and a client certificate to send the credentials of the BlackBerry device to the authentication server.

The BlackBerry device supports EAP-TLS authentication when your organization uses certificates that meet specific requirements on the authentication server and the client for authentication. To configure EAP-TLS authentication, you must install a client certificate and a root certificate on the BlackBerry device that corresponds to the certificate of the authentication server. For more information, see the *BlackBerry Enterprise Server Administration Guide*.

For more information about EAP-TLS authentication, see RFC 2716.

EAP-TTLS authentication

EAP-TTLS authentication can extend EAP-TLS authentication to permit a Wi-Fi® enabled BlackBerry® device to authenticate with the authentication server and access an enterprise Wi-Fi network. When the authentication server uses its certificate to authenticate with the BlackBerry device and open a protected connection to the BlackBerry device, the authentication server uses an authentication protocol over the protected connection to authenticate the BlackBerry device.

The BlackBerry device supports EAP-MS-CHAPv2 and MS-CHAPv2 as second-phase protocols during EAP-TTLS authentication so that the BlackBerry device can exchange credentials with the enterprise Wi-Fi network.

To configure EAP-TTLS authentication, you must install the root certificate on the BlackBerry device that corresponds to the certificate of the authentication server. For more information, see the *BlackBerry Enterprise Server Administration Guide*.

EAP-FAST authentication

EAP-FAST authentication uses PAC to open a TLS connection to a Wi-Fi® enabled BlackBerry® device and verify the supplicant credentials of the BlackBerry device over the TLS connection.

The BlackBerry device supports EAP-MS-CHAPv2 and EAP-GTC as second-phase protocols during EAP-FAST authentication so that the BlackBerry device can exchange authentication credentials with the enterprise Wi-Fi network. The BlackBerry device supports using automatic PAC provisioning with EAP-FAST authentication only.

For more information about EAP-FAST authentication, see RFC 4851.

EAP-SIM authentication

EAP-SIM authentication uses a GSM® SIM card to authenticate a Wi-Fi® enabled BlackBerry® device with an enterprise Wi-Fi network and distribute session keys. EAP-SIM authentication uses a challenge-response method without mutual authentication.

The BlackBerry device supports using EAP-SIM authentication with the credentials on the GSM SIM card only. The user is not required to type or select credentials on the BlackBerry device.

The user identity that EAP-SIM uses for authentication on the BlackBerry device is built from IMSI using the 3GPP® technical specification 3GPP-TS-23.003.

The BlackBerry device can receive at least two challenges from the authentication server to provide stronger authentication.

For more information about EAP-SIM authentication, see RFC 4186.

Encryption keys that a Wi-Fi enabled BlackBerry device supports for use with layer 2 security methods

A Wi-Fi® enabled BlackBerry device supports AES-CCMP encryption keys, TKIP encryption keys, and WEP encryption keys.

The BlackBerry device supports the use of AES-CCMP with the following authentication methods:

- EAP-FAST authentication
- EAP-TLS authentication
- EAP-TTLS authentication
- PEAP authentication
- PSK authentication

The BlackBerry device supports the use of TKIP with the following authentication methods:

- EAP-FAST authentication
- EAP-TLS authentication

- EAP-TTLS authentication
- PEAP authentication
- PSK authentication

For more information about AES-CCMP and TKIP, visit www.ieee.org/portal/site.

EAP authentication methods that a BlackBerry device supports the use of CCKM with

A Wi-Fi® enabled BlackBerry® device supports the use of CCKM with all supported EAP authentication methods to improve roaming between wireless access points. The BlackBerry device does not support the use of CCKM with the Cisco® CKIP encryption algorithm or the AES-CCMP encryption algorithm.

Using certificates with PEAP authentication, EAP-TLS authentication, or EAP-TTLS authentication

If your organization uses PEAP authentication, EAP-TLS authentication, or EAP-TTLS authentication to protect the wireless access points for your organization's enterprise Wi-Fi® network, a Wi-Fi enabled BlackBerry® device must authenticate mutually with an access point using an authentication server. To generate the certificates that the BlackBerry device and authentication server use to authenticate with each other, you require a certification authority.

For PEAP authentication, EAP-TLS authentication, or EAP-TTLS authentication to be successful, the BlackBerry device must trust the certificate of the authentication server. The BlackBerry device does not trust the certificate of the authentication server automatically. Before you can configure the BlackBerry device to trust the certificate of the authentication server, the following conditions must exist:

- A certification authority that the BlackBerry device and authentication server mutually trust must generate the certificate of the authentication server and a certificate for the BlackBerry device.
- The BlackBerry device must store the root certificates in the certificate chain for the certificate of the authentication server.

Each BlackBerry device stores a list of root certificates that are issued by certification authorities that it explicitly trusts.

Protecting a third-party application on a BlackBerry device 18

Creating a third-party application for a BlackBerry device

A developer can create a third-party application for a Java® based BlackBerry® device using the BlackBerry® Java® Development Environment. A third-party application can perform the following actions on a BlackBerry device:

- communicate and share persistent storage with other applications
- access user data such as calendar entries, email messages, and contacts

By default, a user can download a third-party application to a BlackBerry device over the wireless network using the BlackBerry® Browser. You can also send a third-party application to the BlackBerry device over the wireless network so that a user can install it on the BlackBerry device.

Specifying the resources third-party applications can access on a BlackBerry device

You can specify which applications a user can download and install on a BlackBerry® device and the resources on the BlackBerry device that the applications can access. When you control the applications that a user can install and limit the resources that the applications can access, you can help protect the BlackBerry device from malware. You can also help prevent damage to the BlackBerry device, applications, BlackBerry device data, or your organization's network.

You can use application control policy rules and code signing to control application access to the resources and to help prevent malware on the BlackBerry device.

For more information, see *Protecting the BlackBerry Device Platform Against Malware*.

Managing third-party applications on a BlackBerry device using application control policy rules

You can use application control policy rules to specify whether a user can install a third-party application on a BlackBerry® device and to specify the permissions of the application.

You can use application control policy rules to specify whether an application can access the following items on the BlackBerry device the following items:

- data or applications (for example, messaging, phone)
- BlackBerry device key store

- User Authenticator API, which permits the registration of drivers so that a user can unlock the BlackBerry device using two-factor authentication

You can also use application control policy rules to specify the types of connections that the application that is running on the BlackBerry device can open (for example, local, internal, and external connections).

For example, you can create an application control policy rule that prevents an application from opening connections to internal servers. When you assign an application control policy to a software configuration and assign the software configuration to a user account or group, the user might not be able to use all of the features of a third-party application that is included in the software configuration. When you assign the application control policy rule to a software configuration and assign the software configuration to a group, the BlackBerry® Enterprise Server limits permitted application behavior to a subset of user accounts that it trusts.

The BlackBerry device revokes the application control policy and resets itself if the permissions for an application that the application control policy is applied to become more restrictive. A BlackBerry device that is running BlackBerry® Device Software version 4.1 or later permits the user to make permissions more restrictive, but never less restrictive than, the permissions that you specify.

Managing BlackBerry Java Applications on a BlackBerry device using code signing

Before a BlackBerry® Java® Application can use BlackBerry device APIs that include sensitive packages, classes, or methods, Research In Motion requires that the RIM® signing authority system digitally sign the application. Sensitive packages, classes, or methods are APIs that impact device data or permit an application to communicate with another application.

The RIM signing authority system uses public key cryptography to authorize and authenticate the application code. The developer must visit www.blackberry.com/developers/downloads/jde/api.shtml to register the application with the RIM signing authority system so that the application can access the controlled APIs and use the BlackBerry® Signing Authority Tool. The BlackBerry Signing Authority Tool is a component of the BlackBerry® Java® Development Environment that permits an application to request, receive, and verify a digital signature from RIM.

If a developer creates a third-party API that controls access to resources and applications on the BlackBerry device, the developer can act as a signing authority for the third-party API. The developer can download and install the BlackBerry Signing Authority Tool and permit other developers to register with the BlackBerry Signing Authority Tool so that the applications that other developers create can access the third-party API. Developers who register with the RIM signing authority system can use the BlackBerry Signing Authority Tool to request, receive, and verify digital signatures for applications.

MIDlets (also known as applications that use standard MIDP APIs and CLDC APIs only) cannot write to the BlackBerry device memory, access the memory of other applications, or access the persistent data of other MIDlets unless the RIM signing authority system digitally signed them.

For more information about code signing and third-party applications, see the *BlackBerry Signing Authority Tool Administration Guide*.

Permitting a third-party application to encode data on a BlackBerry device

A developer can use the Transcoder API to create an encoding scheme for data that is sent between a BlackBerry® Enterprise Server and BlackBerry device. The Transcoder API is part of the BlackBerry® Java® Development Environment. The BlackBerry Enterprise Server and BlackBerry device can use the encoding scheme to encode and decode all gateway message envelope packets that the BlackBerry Enterprise Server and BlackBerry device send between each other. The encoding scheme prepends a transcoder ID to the encoded data. The BlackBerry® Enterprise Solution encrypts the encoded data using BlackBerry transport layer encryption.

Before an application can access the Transcoder API, the BlackBerry® Signing Authority Tool must digitally sign the .cod file. The BlackBerry Signing Authority Tool uses the key of the RIM® Cryptographic API to authorize and authenticate the Transcoder implementation code.

If the RIM Cryptographic API does not support an algorithm, the developer can use the Transcoder API to add the algorithm to the encoding schemes. The BlackBerry Enterprise Solution applies the encoding schemes to any outgoing data that the BlackBerry transport layer encryption applies to. By default, the Transcoder API supports all algorithms that the RIM Cryptographic API supports.

If you permit the application to use the Transcoder API on the BlackBerry device, and if the application is not working correctly, the application might affect the security, usability, and performance of the BlackBerry Enterprise Solution. It might also cause the loss of BlackBerry device data.

To permit the BlackBerry Enterprise Server and BlackBerry device to use the encoding scheme, you must specify the hash of the .cod file of the application in the Security Transcoder Cod File Hashes IT policy rule. For more information about using this IT policy rule, see the *BlackBerry Enterprise Server Policy Reference Guide*.

Removing third-party applications when a user deletes all BlackBerry device data

If a user clicks Wipe Device, Wipe Handheld, or Security Wipe in the security options on a BlackBerry® device, the user can select the Include third party applications option or the User Installation Application option at the same time. If the user selects this option, when the BlackBerry device permanently deletes its stored user data, it also removes all applications and application data.

RIM Cryptographic API

19

The RIM® Cryptographic API that is on a BlackBerry® device and in the BlackBerry® Java® Development Environment consists of a Java interface that includes an encryption algorithm, a key agreement scheme, a signature scheme algorithm, a key generation algorithm, a message authentication code, cipher suites, a message digest, and a hash code.

A developer can use the BlackBerry JDE to access the RIM Cryptographic API to create an application that can run on the BlackBerry device. The developer is not required to change or access the encryption code directly because all calls to the native C++ encryption code are sent through the Java code.

Research In Motion uses code signing to authorize and authenticate an application and permit it to run on the BlackBerry device. Code signing is also used to control the ability of the application to access the RIM Cryptographic API.

Related topics

Advanced Security SD cards, 96

Cryptographic algorithms and cryptographic codes that the RIM Cryptographic API supports

Symmetric block algorithms that the RIM Cryptographic API supports

Symmetric block algorithms use PKCS #5 for padding. The RIM® Cryptographic API supports the CBC, CFB, ECB, OFB, and X modes for all algorithms. The RIM Cryptographic API implements the modes separately from the symmetric block algorithms.

Algorithm	Key length (bits)
AES	128, 192, and 256
CAST5	128
DES	56
RC2	8 to 1024
RC5®	0 to 2040
Skipjack	80
Triple DES	112 and 168

Stream encryption algorithms that the RIM Cryptographic API supports

The RIM® Cryptographic API supports the ARC4 algorithm, with an unlimited key length, as the symmetric stream encryption algorithm.

The RIM Cryptographic API supports the ECIES algorithm, with an unlimited key length (160 bits to 571 bits for seeding), as the asymmetric stream encryption algorithm.

Asymmetric encryption algorithms that the RIM Cryptographic API supports

Algorithm	Key length (bits)	Type
El Gamal	512 to 4096	discrete logarithm
RSA® raw	512 to 4096	integer factorization
RSA with OAEP formatting	512 to 4096	integer factorization
RSA with PKCS #1 formatting (versions 1.5 and 2.0)	512 to 4096	integer factorization

Key agreement scheme algorithms that the RIM Cryptographic API supports

Algorithm	Key length (bits)	Type
Diffie-Hellman	512 to 4096	discrete logarithm
ECDH	160 to 571	(Elliptic Curve) discrete logarithm
ECMQV	160 to 571	(Elliptic Curve) discrete logarithm
KEA	1024	discrete logarithm

Signature scheme algorithms that the RIM Cryptographic API supports

If the signature scheme algorithm that a developer wants to use is the RSA® algorithm using ANSI® X9.31, ANSI X9.31 uses one of the following algorithms for the required message digest code: SHA-1, SHA-256, SHA-384, SHA-512, or RIPEMD-160.

Algorithm	Key length (bits)	Type
DSA	512 to 1024	discrete logarithm
ECDSA	160 to 571	(Elliptic Curve) discrete logarithm
ECNR	160 to 571	(Elliptic Curve) discrete logarithm
RSA® using ANSI X9.31	512 to 4096	integer factorization
RSA using PKCS #1 (versions 1.5 and 2.0)	512 to 4096	integer factorization
RSA using PSS	512 to 4096	integer factorization

Key generation algorithms that the RIM Cryptographic API supports

Algorithm	Key length (bits)	Type
Diffie-Hellman	512 to 4096	discrete logarithm
DSA	512 to 1024	discrete logarithm
Elliptic Curve	160 to 571	(Elliptic Curve) discrete logarithm
RSA®	512 to 2048	integer factorization

Message authentication codes that the RIM Cryptographic API supports

Code	Key length (bits)
CBC-MAC	variable (block cipher key length)
HMAC	variable

Message digest codes that the RIM Cryptographic API supports

Code	Digest length (bits)
MD2	128
MD4	128
MD5	128
RIPEMD	128, 160
SHA	160, 224, 256, 384, 512

TLS and WTLS protocols that the RIM Cryptographic API supports

The RIM® Cryptographic API supports the cipher suite components for the TLS protocol and WTLS protocol that apply only to direct mode SSL/TLS and WTLS.

Cipher suites for the key establishment algorithm that the RIM Cryptographic API supports

Direct mode SSL	Direct mode TLS	WTLS
DH_anon	DH_anon	RSA® _768, DH_anon, DH_anon_512, DH_anon_768
DH_anon_EXPORT	DH_anon_EXPORT	RSA_anon_512
DHE_DSS	DHE_DSS	RSA_512
DHE_DSS_EXPORT	DHE_DSS_EXPORT	RSA_anon_768
RSA	RSA	RSA
RSA_EXPORT	RSA_EXPORT	RSA_anon

Symmetric algorithms that the RIM Cryptographic API supports

Direct mode SSL	Direct mode TLS	WTLS
DES	ARC4-128	RC5® -64
DES-40	ARC4-56	RC5-56
ARC4-128	DES	RC5-128
ARC4-128	Triple DES	DES-40
ARC4-128	AES-128	DES
ARC4-128	AES-256, ARC4-128	Triple DES
ARC4-40	ARC4-40	RC5-40
Triple DES	DES-40	RC5

Hash algorithms that the RIM Cryptographic API supports

Direct mode SSL	Direct mode TLS	WTLS
MD5	MD5	SHA
SHA-1	SHA-1	SHA-40, SHA-80, MD5, MD5-40, MD5-80

Limitations of RIM Cryptographic API support for cipher suites for the key establishment algorithm

The RIM® Cryptographic API implementation of the TLS protocol and WTLS protocol supports the use of the RSA® public key algorithm, DSA public key algorithm, and Diffie-Hellman key exchange algorithm, with the following limitations.

Cipher suite type	Typical component limitation
export	• RSA and Diffie-Hellman: 1024 bytes or less • elliptic curve: 163 bytes or less
non-export	• non elliptic curve operations: 4096 bytes • elliptic curve operations: 571 bytes

Limitations to non-export cipher suite types are due to the computational constraints of a BlackBerry® device.

Related resources

20

Resource	Information
BlackBerry Enterprise Server Feature and Technical Overview	• understanding BlackBerry® Enterprise Server architecture
BlackBerry Enterprise Server Installation Guide	• understanding system requirements • performing preinstallation tasks • installing the BlackBerry Enterprise Server
BlackBerry Enterprise Server Administration Guide	• generating and changing device transport keys • configuring extended messaging encryption • managing security • protecting lost or stolen BlackBerry devices
BlackBerry Enterprise Server Policy Reference Guide	• understanding BlackBerry Enterprise Server IT policy rules and application control policy rules • using IT policies and application control policies
BlackBerry Signing Authority Tool Administrator Guide	• understanding the BlackBerry® Signing Authority Tool implementation of public key cryptography • installing, configuring, and managing the BlackBerry Signing Authority Tool • restricting access to APIs
BlackBerry Java Development Environment Fundamentals Guide	• understanding BlackBerry APIs in the BlackBerry® Java® Development Environment • understanding APIs, classes, and methods with limited access • retrieving custom IT policy rules from the IT policy API • installing applications using the BlackBerry® Desktop Software • publishing applications over the wireless network
BlackBerry Java Development Environment Development Guide	• using controlled APIs • using code signatures
BlackBerry Smart Card Reader Security Technical Overview	• understanding highly secure pairings between the BlackBerry device and BlackBerry® Smart Card Reader • understanding how the initial key establishment protocol works • understanding how the connection key establishment protocol works

Resource	Information
Enforcing Encryption of Internal and External File Systems on BlackBerry Devices Technical Overview	• understanding which data items BlackBerry devices encrypt by default • using encryption to protect stored files in the on-board device memory and media cards
Erasing File Systems on BlackBerry Devices Technical Overview	• understanding which data items are deleted from BlackBerry device memory when you or a user deletes the BlackBerry device memory • understanding the different methods of permanently deleting BlackBerry device memory
PGP Support Package for BlackBerry Devices Security Technical Overview	• understanding PGP® security and encryption • using PGP® Universal Server to store and manage PGP keys • searching for and validating PGP keys • sending and receiving PGP messages
Protecting the BlackBerry Device Platform Against Malware	• understanding the default behavior of the BlackBerry device platform • understanding malware vulnerabilities on the BlackBerry device • managing the risk of malware attacks • using BlackBerry® Enterprise Solution tools to contain malware on the BlackBerry device
S/MIME Support Package for BlackBerry Devices Technical Overview	• understanding S/MIME security and encryption • managing S/MIME certificates on the BlackBerry device and a computer
Security for BlackBerry Devices with Bluetooth Wireless Technology	• Bluetooth® wireless technology overview • using and protecting Bluetooth enabled BlackBerry devices • risks of using Bluetooth wireless technology on mobile devices
www.blackberry.com/security	• understanding BlackBerry Enterprise Solution security

Glossary

21

3GPP
Third Generation Partnership Project

AES
Advanced Encryption Standard

AES-CCMP
Advanced Encryption Standard Counter Mode CBCMAC Protocol

ANSI
American National Standards Institute

API
application programming interface

ARC4
alleged RC4 (algorithm)

ASCII
American Standard Code for Information Interchange

BlackBerry device key
The BlackBerry device key is a randomly generated key that a BlackBerry device uses to encrypt data on media cards.

BlackBerry device key store
The BlackBerry device key store stores certificates, key pairs, and PGP® keys that a BlackBerry device can use to help protect messages, access web sites, and connect to an enterprise Wi-Fi® network. To access the items in the key store, the user must type a key store password.

BlackBerry device memory
The BlackBerry device memory consists of the NV store, flash memory, RAM, on-board device memory, and BlackBerry device key store.

BlackBerry inter-process protocol
The BlackBerry inter-process protocol is a Research In Motion® proprietary protocol that generates the session key that BlackBerry® Enterprise Solution components such as the BlackBerry® Enterprise Server and BlackBerry® Mobile Voice System can use to communicate in a highly securely manner with each other. The BlackBerry inter-process protocol generates the session key based on the secure communication password.

BlackBerry inter-process protocol encryption

BlackBerry inter-process protocol encryption encrypts communication between BlackBerry® Enterprise Solution components to prevent other parties from viewing the data that the components send between each other.

BlackBerry MDS
BlackBerry® Mobile Data System

BlackBerry MDS security protocol
The BlackBerry MDS security protocol is a Research In Motion® proprietary protocol that helps protect the data that a BlackBerry device, the BlackBerry MDS Connection Service, and the BlackBerry MDS Integration Service send between each other.

BlackBerry MVS
BlackBerry® Mobile Voice System

BlackBerry transport layer encryption
BlackBerry transport layer encryption (formerly known as standard BlackBerry encryption) uses a symmetric key encryption algorithm to help protect data that is in transit between a BlackBerry device and the BlackBerry® Enterprise Server when the data is outside an organization's firewall.

CA
certification authority

CAC
Common Access Card

CAST
Computer Assisted Seriation Test

CBC
cipher block chaining

CCKM
Cisco® Centralized Key Management

CFB
cipher feedback

CHAP
Challenge Handshake Authentication Protocol

CKIP
Cisco® Key Integrity Protocol

CLDC
Connected Limited Device Configuration

code-signing keys
Code-signing keys are the keys that are stored on media cards that sign files so that a user can install and run the files on a BlackBerry device.

content protection
Content protection protects user data on a locked BlackBerry device by encrypting the user data using the content protection key and ECC private key.

content protection key
The device transport key (formerly known as the master encryption key) is unique to a BlackBerry device. The BlackBerry device and BlackBerry® Enterprise Server use the device transport key to encrypt the message keys.

DEMA
Differential Electromagnetic Analysis

DES
Data Encryption Standard

device transport key
The device transport key (formerly known as the master encryption key) is unique to a BlackBerry device. The BlackBerry device and BlackBerry® Enterprise Server use the device transport key to encrypt the message keys.

DH
Diffie-Hellman

DHE
Diffie-Hellman Ephemeral

DoS
denial of service

DPA
Differential Power Analysis

DSA
Digital Signature Algorithm

DSML
Directory Service Markup Language

DSML certificate server
A BlackBerry® device uses a DSML certificate server to search for and download certificates.

DSS
Digital Signature Standard

EAP
Extensible Authentication Protocol

EAPoL
Extensible Authentication Protocol over LAN

EAP-FAST
Extensible Authentication Protocol Flexible Authentication via Secure Tunneling

EAP-GTC
Extensible Authentication Protocol Generic Token Card

EAP-MS-CHAP
Extensible Authentication Protocol Microsoft® Challenge Handshake Authentication Protocol

EAP-SIM
Extensible Authentication Protocol Subscriber Identity Module

EAP-TLS
Extensible Authentication Protocol Transport Layer Security

EAP-TTLS
Extensible Authentication Protocol Tunneled Transport Layer Security

ECB
electronic code book

ECC
Elliptic Curve Cryptography

ECC private key
The ECC private key decrypts the data that a BlackBerry device received when the BlackBerry device was locked.

ECC public key
The ECC public key encrypts the data that a BlackBerry device receives when the BlackBerry device is locked.

ECDH
Elliptic Curve Diffie-Hellman

ECDSA
Elliptic Curve Digital Signature Algorithm

ECIES
Elliptic Curve Integrated Encryption Standard

ECMQV
Elliptic Curve Menezes-Qu-Vanstone

ECNR
Elliptic Curve Nyberg Rueppel

EDE
Encryption-Decryption-Encryption

EDGE
Enhanced Data Rates for Global Evolution

Enterprise Service Policy
The Enterprise Service Policy controls which BlackBerry devices can connect to a BlackBerry® Enterprise Server.

ephemeral key
The ephemeral key encrypts the ECC public key, ECC private key, and content protection key.

FIPS
Federal Information Processing Standards

flash memory
The flash memory is an internal file system on a BlackBerry device that stores application data and user data.

GAN
generic access network

GANC
generic access network controller

global PIN encryption key
The global PIN encryption key is a key that is added to all BlackBerry devices during the manufacturing process. The global PIN encryption key permits BlackBerry devices to encrypt and send PIN messages to each other.

GME
The gateway message envelope (GME) protocol is a Research In Motion proprietary protocol that allows the transfer of compressed and encrypted data between the wireless network and BlackBerry devices. The protocol defines a routing layer that specifies the types of message contents allowed and the addressing information for the data. Gateways and routing components use this information to identify the type and source of the BlackBerry device data, and the appropriate destination service to route the data to.

GPS
Global Positioning System

GSA

General Services Administration

GSM
Global System for Mobile communications®

HMAC
keyed-hash message authentication code

HTTP
Hypertext Transfer Protocol

HTTPS
Hypertext Transfer Protocol over Secure Sockets Layer

IEEE
Institute of Electrical and Electronics Engineers

IMSI
International Mobile Subscriber Identity

initial key establishment protocol
The initial key establishment protocol is a Research In Motion® proprietary protocol that the BlackBerry® Enterprise Solution uses to generate the first device transport key for a BlackBerry device.

IT administration command
An IT administration command is a command that you can send over the wireless network to protect sensitive information on a BlackBerry device or delete all BlackBerry device data.

IP
Internet Protocol

IPSec
Internet Protocol Security

IT policy
An IT policy consists of various IT policy rules that control the security features and behavior of BlackBerry devices, BlackBerry enabled devices, the BlackBerry® Desktop Software, and the BlackBerry® Web Desktop Manager.

IT policy private key
The IT policy private key is a key that the BlackBerry® Enterprise Server uses to sign an IT policy before the BlackBerry Enterprise Server sends the IT policy to a BlackBerry device.

IT policy public key
The IT policy public key is a key that a BlackBerry device uses to authenticate the IT policy that the BlackBerry® Enterprise Server sends.

IT policy rule
An IT policy rule permits you to customize and control the actions that BlackBerry devices, BlackBerry enabled devices, the BlackBerry® Desktop Software, and the BlackBerry® Web Desktop Manager can perform.

JSSE
Java® Secure Socket Extension

KEA
Key Exchange Algorithm

key rollover protocol
The key rollover protocol is a Research In Motion® proprietary protocol that the BlackBerry® Enterprise Solution uses to generate subsequent device transport keys for a BlackBerry device.

LAN
local area network

LDAP
Lightweight Directory Access Protocol

LDAPS
Lightweight Directory Access Protocol over SSL

LEAP
Lightweight Extensible Authentication Protocol

MAC
message authentication code

MAPI
Messaging Application Programming Interface

MCEX
Mobile Commerce Extension

MD5
Message-Digest Algorithm, version 5

message keys
The message keys encrypt the data that is sent to and from a BlackBerry device.

messaging server
A messaging server sends and processes messages and provides collaboration services, such as updating and communicating calendar and address book information.

MIDP
Mobile Information Device Profile

MMS
Multimedia Messaging Service

MS-CHAP
Microsoft Challenge Handshake Authentication Protocol

NAT
network address translation

NIST
National Institute of Standards and Technology

NTFS
New Technology File System

NTLM
NT LAN Manager

NV
nonvolatile

NV store
The NV store is a nonvolatile store that persists in flash memory on a BlackBerry device. Only the operating system of the BlackBerry device can write to it. Third-party applications cannot write to the NV store.

OAEP
Optimal Asymmetric Encryption Padding

OCSP
Online Certificate Status Protocol

OFB
output feedback

PAC
proxy auto-configuration

PBX
Private Branch Exchange

PEAP
Protected Extensible Authentication Protocol

PFS
Perfect Forward Secrecy

persistent store in flash memory
The persistent store in flash memory stores data for a BlackBerry device. By default, third-party applications cannot access the persistent store. When it deletes all device data, the BlackBerry device deletes the data in the persistent store.

PGP/MIME
PGP® Multipurpose Internet Mail Extensions

PIN
personal identification number

PKCS
Public-Key Cryptography Standards

PKI
Public Key Infrastructure

PMK
pairwise master key

POA
Post Office Agent

principal encryption key
The principal encryption key (formerly known as the grand master key) encrypts the device transport key when a BlackBerry device is locked.

PRNG
pseudo-random number generator

PSK
pre-shared key

PSS
Probabilistic Signature Scheme

RC
Rivest's Cipher

remote password reset cryptographic protocol
The remote password reset cryptographic protocol is a Research In Motion® proprietary protocol that permits you to reset the BlackBerry device password when content protection is turned on.

RFC
Request for Comments

RIM signing authority system
The RIM® signing authority system is a collection of servers that sign the boot ROM code for a BlackBerry device during the manufacturing process.

RIPEMD
RACE Integrity Primitives Evaluation Message Digest

RPC
remote procedure call

S/MIME
Secure Multipurpose Internet Mail Extensions

secure communication password
The secure communication password is a password that BlackBerry® Enterprise Solution components use for the BlackBerry inter-process protocol. The secure communication password is designed to prevent a potentially malicious user from viewing the data that the components send to each other.

SEMA
Simple Electromagnetic Analysis

SHA
Secure Hash Algorithm

SIM
Subscriber Identity Module

SMS
Short Message Service

SMTP
Simple Mail Transfer Protocol

SPA
Simple Power Analysis

SPEKE
Simple Password-authenticated Exponential Key Exchange

SRP
Server Routing Protocol

SRP authentication
SRP authentication is an authentication method that the BlackBerry® Enterprise Server and BlackBerry® Infrastructure use to authenticate with each other.

SRP authentication key
The SRP authentication key is a 20-byte shared encryption key that the BlackBerry® Enterprise Server and BlackBerry® Infrastructure use to authenticate with each other during SRP authentication.

SRP ID
The SRP ID is a unique identifier for the BlackBerry® Enterprise Server that the BlackBerry Enterprise Server uses to identify itself to the BlackBerry® Infrastructure during SRP authentication.

SSL
Secure Sockets Layer

TCP
Transmission Control Protocol

TCP/IP
Transmission Control Protocol

TKIP
Temporal Key Integrity Protocol

TLS
Transport Layer Security

Triple DES
Triple Data Encryption Standard

UID
unique identifier

UMA
Unlicensed Mobile Access

VPN
virtual private network

WAP
Wireless Application Protocol

WEP
Wired Equivalent Privacy

WLAN
wireless local area network

WPA
Wi-Fi Protected Access

WTLS
Wireless Transport Layer Security

Provide feedback

22

To provide feedback on this deliverable, visit www.blackberry.com/docsfeedback.

Legal notice

23

©2009 Research In Motion Limited. All rights reserved. BlackBerry®, RIM®, Research In Motion®, SureType®, SurePress™ and related trademarks, names, and logos are the property of Research In Motion Limited and are registered and/or used in the U.S. and countries around the world.

3GPP is a trademark of 3GPP. Bluetooth is a trademark of Bluetooth SIG. ANSI is a trademark of the American National Standards Institute. Cisco is a trademark of Cisco Systems, Inc. Entrust Authority is a trademark of Entrust, Inc. GSM (Global System for Mobile communications) is a trademark of the GSM MOU Association. IBM, Domino, Lotus, Lotus iNotes, and Lotus Notes are trademarks of International Business Machines Corporation. IEEE 802.11, IEEE 802.11i, IEEE 802.1X, and IEEE are trademarks of the Institute of Electrical and Electronics Engineers, Inc. Microsoft, Outlook, and Windows are trademarks of Microsoft Corporation. Netscape is a trademark of Netscape Communication Corporation. Novell and GroupWise are trademarks of Novell, Inc. PGP is a trademark of PGP Corporation. Roxio is a trademark of Sonic Solutions. RC4, RC5, RSA, and RSA SecurID are trademarks of RSA Security. Sun and Java are trademarks of Sun Microsystems, Inc. Wi-Fi Wi-Fi Protected Access, WPA, and WPA2 are trademarks of the Wi-Fi Alliance. All other trademarks are the property of their respective owners.

The BlackBerry smartphone and other devices and/or associated software are protected by copyright, international treaties, and various patents, including one or more of the following U.S. patents: 6,278,442; 6,271,605; 6,219,694; 6,075,470; 6,073,318; D445,428; D433,460; D416,256. Other patents are registered or pending in the U.S. and in various countries around the world. Visit www.rim.com/patents for a list of RIM (as hereinafter defined) patents.

This documentation including all documentation incorporated by reference herein such as documentation provided or made available at www.blackberry.com/go/docs is provided or made accessible "AS IS" and "AS AVAILABLE" and without condition, endorsement, guarantee, representation, or warranty of any kind by Research In Motion Limited and its affiliated companies ("RIM") and RIM assumes no responsibility for any typographical, technical, or other inaccuracies, errors, or omissions in this documentation. In order to protect RIM proprietary and confidential information and/or trade secrets, this documentation may describe some aspects of RIM technology in generalized terms. RIM reserves the right to periodically change information that is contained in this documentation; however, RIM makes no commitment to provide any such changes, updates, enhancements, or other additions to this documentation to you in a timely manner or at all.

This documentation might contain references to third-party sources of information, hardware or software, products or services including components and content such as content protected by copyright and/or third-party web sites (collectively the "Third Party Products and Services"). RIM does not control, and is not responsible for, any Third Party Products and Services including, without limitation the content, accuracy, copyright compliance, compatibility, performance, trustworthiness, legality, decency, links, or any other aspect of Third Party Products and Services. The inclusion of a reference to Third Party Products and Services in this documentation does not imply endorsement by RIM of the Third Party Products and Services or the third party in any way.

EXCEPT TO THE EXTENT SPECIFICALLY PROHIBITED BY APPLICABLE LAW IN YOUR JURISDICTION, ALL CONDITIONS, ENDORSEMENTS, GUARANTEES, REPRESENTATIONS, OR WARRANTIES OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION, ANY CONDITIONS, ENDORSEMENTS, GUARANTEES, REPRESENTATIONS OR WARRANTIES OF DURABILITY, FITNESS FOR A PARTICULAR PURPOSE OR USE, MERCHANTABILITY, MERCHANTABLE QUALITY, NON-INFRINGEMENT, SATISFACTORY QUALITY, OR TITLE, OR ARISING FROM A STATUTE OR CUSTOM OR A COURSE OF DEALING OR USAGE OF TRADE, OR RELATED TO THE DOCUMENTATION OR ITS USE, OR PERFORMANCE OR NON-PERFORMANCE OF ANY SOFTWARE, HARDWARE, SERVICE, OR ANY THIRD PARTY PRODUCTS AND SERVICES REFERENCED HEREIN, ARE

HEREBY EXCLUDED. YOU MAY ALSO HAVE OTHER RIGHTS THAT VARY BY STATE OR PROVINCE. SOME JURISDICTIONS MAY NOT ALLOW THE EXCLUSION OR LIMITATION OF IMPLIED WARRANTIES AND CONDITIONS. TO THE EXTENT PERMITTED BY LAW, ANY IMPLIED WARRANTIES OR CONDITIONS RELATING TO THE DOCUMENTATION TO THE EXTENT THEY CANNOT BE EXCLUDED AS SET OUT ABOVE, BUT CAN BE LIMITED, ARE HEREBY LIMITED TO NINETY (90) DAYS FROM THE DATE YOU FIRST ACQUIRED THE DOCUMENTATION OR THE ITEM THAT IS THE SUBJECT OF THE CLAIM.

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW IN YOUR JURISDICTION, IN NO EVENT SHALL RIM BE LIABLE FOR ANY TYPE OF DAMAGES RELATED TO THIS DOCUMENTATION OR ITS USE, OR PERFORMANCE OR NON-PERFORMANCE OF ANY SOFTWARE, HARDWARE, SERVICE, OR ANY THIRD PARTY PRODUCTS AND SERVICES REFERENCED HEREIN INCLUDING WITHOUT LIMITATION ANY OF THE FOLLOWING DAMAGES: DIRECT, CONSEQUENTIAL, EXEMPLARY, INCIDENTAL, INDIRECT, SPECIAL, PUNITIVE, OR AGGRAVATED DAMAGES, DAMAGES FOR LOSS OF PROFITS OR REVENUES, FAILURE TO REALIZE ANY EXPECTED SAVINGS, BUSINESS INTERRUPTION, LOSS OF BUSINESS INFORMATION, LOSS OF BUSINESS OPPORTUNITY, OR CORRUPTION OR LOSS OF DATA, FAILURES TO TRANSMIT OR RECEIVE ANY DATA, PROBLEMS ASSOCIATED WITH ANY APPLICATIONS USED IN CONJUNCTION WITH RIM PRODUCTS OR SERVICES, DOWNTIME COSTS, LOSS OF THE USE OF RIM PRODUCTS OR SERVICES OR ANY PORTION THEREOF OR OF ANY AIRTIME SERVICES, COST OF SUBSTITUTE GOODS, COSTS OF COVER, FACILITIES OR SERVICES, COST OF CAPITAL, OR OTHER SIMILAR PECUNIARY LOSSES, WHETHER OR NOT SUCH DAMAGES WERE FORESEEN OR UNFORESEEN, AND EVEN IF RIM HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW IN YOUR JURISDICTION, RIM SHALL HAVE NO OTHER OBLIGATION, DUTY, OR LIABILITY WHATSOEVER IN CONTRACT, TORT, OR OTHERWISE TO YOU INCLUDING ANY LIABILITY FOR NEGLIGENCE OR STRICT LIABILITY.

THE LIMITATIONS, EXCLUSIONS, AND DISCLAIMERS HEREIN SHALL APPLY: (A) IRRESPECTIVE OF THE NATURE OF THE CAUSE OF ACTION, DEMAND, OR ACTION BY YOU INCLUDING BUT NOT LIMITED TO BREACH OF CONTRACT, NEGLIGENCE, TORT, STRICT LIABILITY OR ANY OTHER LEGAL THEORY AND SHALL SURVIVE A FUNDAMENTAL BREACH OR BREACHES OR THE FAILURE OF THE ESSENTIAL PURPOSE OF THIS AGREEMENT OR OF ANY REMEDY CONTAINED HEREIN; AND (B) TO RIM AND ITS AFFILIATED COMPANIES, THEIR SUCCESSORS, ASSIGNS, AGENTS, SUPPLIERS (INCLUDING AIRTIME SERVICE PROVIDERS), AUTHORIZED RIM DISTRIBUTORS (ALSO INCLUDING AIRTIME SERVICE PROVIDERS) AND THEIR RESPECTIVE DIRECTORS, EMPLOYEES, AND INDEPENDENT CONTRACTORS.

IN ADDITION TO THE LIMITATIONS AND EXCLUSIONS SET OUT ABOVE, IN NO EVENT SHALL ANY DIRECTOR, EMPLOYEE, AGENT, DISTRIBUTOR, SUPPLIER, INDEPENDENT CONTRACTOR OF RIM OR ANY AFFILIATES OF RIM HAVE ANY LIABILITY ARISING FROM OR RELATED TO THE DOCUMENTATION.

Prior to subscribing for, installing, or using any Third Party Products and Services, it is your responsibility to ensure that your airtime service provider has agreed to support all of their features. Some airtime service providers might not offer Internet browsing functionality with a subscription to the BlackBerry® Internet Service. Check with your service provider for availability, roaming arrangements, service plans and features. Installation or use of Third Party Products and Services with RIM's products and services may require one or more patent, trademark, copyright, or other licenses in order to avoid infringement or violation of third party rights. You are solely responsible for determining whether to use Third Party Products and Services and if any third party licenses are required to do so. If required you are responsible for acquiring them. You should not install or use Third Party Products and Services until all necessary licenses have been acquired. Any Third Party Products and Services that are provided with RIM's products and services are provided as a convenience to you and are provided "AS IS" with no express or implied conditions, endorsements, guarantees, representations, or warranties of any kind by RIM and RIM assumes no liability whatsoever, in relation

thereto. Your use of Third Party Products and Services shall be governed by and subject to you agreeing to the terms of separate licenses and other agreements applicable thereto with third parties, except to the extent expressly covered by a license or other agreement with RIM.

Certain features outlined in this documentation require a minimum version of BlackBerry® Enterprise Server, BlackBerry® Desktop Software, and/or BlackBerry® Device Software.

The terms of use of any RIM product or service are set out in a separate license or other agreement with RIM applicable thereto. NOTHING IN THIS DOCUMENTATION IS INTENDED TO SUPERSEDE ANY EXPRESS WRITTEN AGREEMENTS OR WARRANTIES PROVIDED BY RIM FOR PORTIONS OF ANY RIM PRODUCT OR SERVICE OTHER THAN THIS DOCUMENTATION.

Certain features outlined in this documentation might require additional development or Third Party Products and Services for access to corporate applications.

Research In Motion Limited
295 Phillip Street
Waterloo, ON N2L 3W8
Canada

Research In Motion UK Limited
Centrum House
36 Station Road
Egham, Surrey TW20 9LF
United Kingdom

Published in Canada